

(19) 世界知的所有權機關
國際事務局



(43) 國際公開日
2003 年 9 月 12 日 (12.09.2003)

PCT

(10) 国際公開番号
WO 03/075163 A1

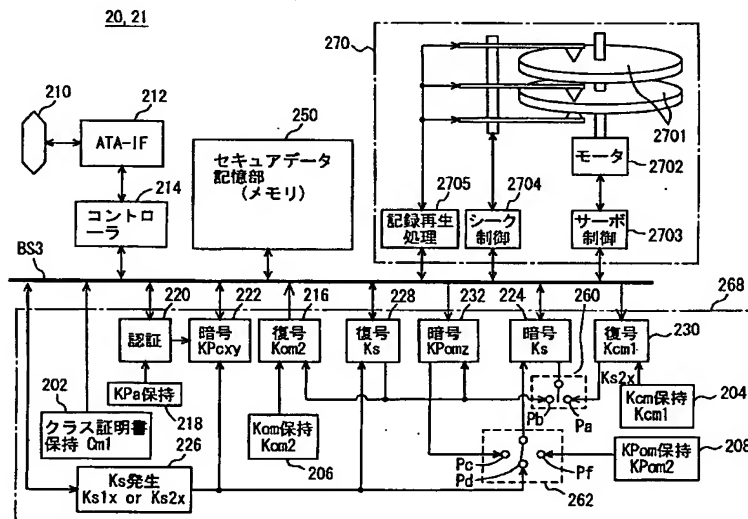
- | | |
|--|------------------------------|
| (51) 国際特許分類 ⁷⁾ : | G06F 12/14, 3/06 |
| (21) 国際出願番号: | PCT/JP03/02525 |
| (22) 国際出願日: | 2003 年3 月4 日 (04.03.2003) |
| (25) 国際出願の言語: | 日本語 |
| (26) 国際公開の言語: | 日本語 |
| (30) 優先権データ:
特願2002-59179 | 2002 年3 月5 日 (05.03.2002) JP |
| (71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; | |

〒570-8677 大阪府 守口市 京阪本通2丁目5番5号
Osaka (JP). シャープ株式会社 (SHARP KABUSHIKI
KAISHA) [JP/JP]; 〒545-8522 大阪府 大阪市 阿倍野
区長池町2番22号 Osaka (JP). 日本ビクター株
式会社 (VICTOR COMPANY OF JAPAN, LIMITED)
[JP/JP]; 〒221-8528 神奈川県 横浜市 神奈川区守屋町
3丁目12番地 Kanagawa (JP). パイオニア株式会社
(PIONEER CORPORATION) [JP/JP]; 〒153-8654 東京
都 目黒区 目黒1丁目4番1号 Tokyo (JP). 株式会社
日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京
都 千代田区 神田駿河台四丁目6番地 Tokyo (JP).
フェニックステクノロジーズ株式会社 (PHOENIX
TECHNOLOGIES, K.K.) [JP/JP]; 〒100-0005 東京
都 千代田区 丸の内1丁目3番地1 東京銀行協会ビル

[統葉有]

(54) Title: DATA STORING DEVICE

(54) 発明の名称: データ記憶装置



214...CONTROLLER

250...SECURE DATA STORING PART (MEMORY)

2705...RECORD/REPRODUCTION PROCESSINGS

2704...SEEK CONTROL

2702...MOTOR

2703...SERVO CONTROL

202...CLASS CERTIFICATE HOLDING

226...KS OCCURRENCE

Ks1x OR Ks2x

218...KPa HOLDING

220 AUTHENTICATING

220...AUTHENTICATING

222...ENCRYPTING

KPcxv

216...DECODING Kom2

206 KOM HOLDING Kom2

228 DECODING KEYS

232 ENCRYPTING KBomz

232...ENCRYPTING
234...ENCRYPTING224...ENCRYPTING K_s
228...DECRYPTING K_{s-1}

230...DECODING Kcm1

204...Kcm HOLDING Kcm1

208...KPom HOLDING KPom2

データ記憶部（250）内においてLBA（アドレス情報）によって管理され、また、送受信処理中のライセンス（LIC）が格納されるLBAがログとしてセキュアデータ記憶部（250）内のログメモリ（25

[續葉有]

(57) Abstract: A controller (214) in an HD (hard disc) (20,21) serving as a data storing device causes a secure data storing part (250) to store therein a license (LIC) including a content key (K_C) for decoding encrypted content data ($E(K_C, D_C)$). The license (LIC) is managed by LBA (address information) in the secure data storing part (250). An LBA in which a license (LIC) being subject to transmission/reception processing is included is stored, as a log, in a log memory (250B) in the secure data storing part (250). When any trouble occurs during transmission/reception processing, the license (LIC) that was being subjected to the transmission/reception processing is identified based on the LBA stored in the log memory (250B).

(57) 要約: データ記録装置としてのHD (ハードディスク) (20, 21) におけるコントローラ (214) は、暗号化コンテンツデータE (Kc, Dc) を復号するためのコンテンツ鍵 (Kc) などを含むライセンス (LIC) をセキュアデータ記憶部 (250) に記憶する。ライセンス (LIC) は、セキュア



1 4 階 Tokyo (JP). 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区上小田中 4 丁目 1 番 1 号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてののみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府 守口市 京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内 Osaka (JP). 大野 良治 (OHNO, Ryoji) [JP/JP]; 〒545-8522 大阪府 大阪市 阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内 Osaka (JP). 大石 剛士 (OHISHI, Takeo) [JP/JP]; 〒221-8528 神奈川県 横浜市 神奈川区 守屋町 3 丁目 1 2 番地 日本ビクター株式会社内 Kanagawa (JP). 戸崎 明宏 (TOZAKI, Akihiro) [JP/JP]; 〒359-8522 埼玉県 所沢市 花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内 Saitama (JP). 多田 謙一郎 (TADA, Kenichiro) [JP/JP]; 〒359-8522 埼玉県 所沢市 花園 4 丁目 2 6 1 0 番地 パイオニア株式会社 所沢工場内 Saitama (JP). 平井 達哉 (HIRAI, Tatsuya) [JP/JP]; 〒215-0013 神奈川県 川崎市 麻生区 王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内 Kanagawa (JP). 津留 雅文 (TSURU, Masafumi) [JP/JP]; 〒100-0005 東京都 千代田区 丸の内 1 丁目 3 番地 1 東京銀行協会ビル 1 4 階 フェニックステクノロジー株式会社内 Tokyo (JP). 長谷部 高行 (HASEBE, Takayuki) [JP/JP]; 〒211-8588 神奈川県 川崎市 中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府 大阪市 北区南森町 2 丁目 1 番 2 9 号 三井住友銀行南森町ビル 深見特許事務所 Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

データ記憶装置

5 技術分野

この発明は、デジタルデータ化されたコンテンツデータに対する著作権保護を可能とするデータ配信システムにおけるデータ記憶装置に関し、特に、コンテンツデータを暗号化した暗号化コンテンツデータの再生に際して必要とされるライセンス（復号鍵および利用規則）を安全に入出力し、かつ、多数のライセンスを記憶することができ、さらには、保護を必要とする機密データを安全に入出力し、かつ、機密データの入出力の中断から安全に入出力を再開できるデータ記憶装置に関する。

背景技術

15 近年、インターネット等のデジタル通信網の進歩により、個人端末から各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このようなデジタル通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のようなデジタル通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このようなデジタル通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツデータが伝送される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

25 一方で、著作権保護の目的を最優先して、急拡大するデジタル通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの配信に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えてみると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

しかも、CDからMDへ音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽データをコピーすることは、著作権保護のために機器の構成上できないようになっている。

このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

同様に、デジタル通信網を通じて公衆に送信される音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手にコピーされることを防止することが必要となる。

そこで、デジタル通信網を介したデータ配信システムとして、配信サーバから携帯電話機などの端末装置に装着されたデータ記憶装置としてのメモリカードに対してコンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、認証された証明書を配信サーバが受信したことを確認した上で、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのコンテンツ鍵とをメモリカードに対して送信する。そして、暗号化コンテンツデータやコンテンツ鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッション鍵を発生させ、その発生させたセッション鍵によって公開鍵で暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

最終的に、配信サーバは、メモリカード個々の公開鍵によって暗号化され、さらにセッション鍵によって暗号化したコンテンツ鍵と、暗号化コンテンツデータとをメモリカードへ送信する。そして、メモリカードは、受信したコンテンツ鍵と暗号化コンテンツデータとをメモリに記憶する。この際、ライセンスは、安全性が確保されるライセンス記憶部に記憶される。

そして、ユーザは、メモリカードに記憶した暗号化コンテンツデータを再生するときは、メモリカードを専用の再生回路を備えた再生端末に接続し、その暗号化コンテンツデータを再生して楽しむことができる。

このようなシステムにおいて、コンテンツ供給者あるいは著作権者によって暗号化コンテンツデータの再生や複製に関する利用方法が指示できるように利用規則を定め、この利用規則をコンテンツ鍵とともに配信し、各機器が利用規則に従って処理を行なうことができるようになっている。

利用規則には、メモリカード間のライセンスの複製・移動に関する規則、再生回数の制限などのコンテンツ鍵をメモリカードから出力する場合の規則や、再生されたコンテンツの取扱いに関する規則が規定されている。

上述したようなデータ配信システムにおいては、暗号化コンテンツデータとライセンスとが、配信サーバとメモリカードとの間や、あるいはメモリカードと再生端末との間などで送受信される。ここで、ライセンスとは、コンテンツ鍵や、利用規則、ライセンスを特定するためのライセンスID、あるいは上述したコンテンツの利用規則などを総称するものである。そして、このライセンスこそが著作権を保護する目的からセキュリティに十分配慮して送受信されるべきものである。

ここで、ライセンスを装置間で送受信する際に、通常送受信処理中であれば、送信側と受信側とにおいて送受信を行なっているライセンスを互いに認識し、ライセンスは両装置の間を問題なく送受信されるが、ライセンスの送受信中にいずれかの装置あるいは通信路において異常（たとえば、装置の電源の遮断など）が発生すると、送受信中のライセンスが消失してしまうことがある。

たとえば、メモリカード間でライセンスの送受信を行なう場合、利用規則によってライセンスの複製に制限のないコンテンツを除いては、著作権保護の観点か

ら、送信側のメモリカードおよび受信側のメモリカードの両装置において同時に同一のライセンスが利用可能な状態で記憶できない構成となっている。すなわち、送信側のメモリカードに記憶されているライセンスは、受信側のメモリカードに対してライセンスを出力すると同時に利用できないものとなる必要がある。この

5 ような場合、一時的にはあるが、両メモリカードのいずれにも利用可能な状態でライセンスが記憶されていない状態が発生する。このような状態のときに送受信処理が中断すると、送信中のライセンスが消失してしまうのである。配信サーバからライセンスを受信する場合においても、同様にライセンスの消失の危険性がある。したがって、ライセンスの送受信が中断した場合に、その中断した送受信処理においてライセンスが消失したか否かを確認し、ライセンスが消失した場合には、消失したライセンスの復元または再送信処理をいかに適切に行なうかが重要になってくる。そして、メモリカードには、ライセンスの消失を確認するために、送受信中であった送受信処理とライセンスとを特定するためのログ情報を効率的に記録しておく必要がある。また、メモリカードには、当該ライセンスが

10 記憶されているか否かを確認する機能も必要となる。

一方、近年、そして今後さらなる飛躍的進歩が確実視されるIT技術の進展に伴う通信技術の高度化や情報量の増大などがあいまって、上述したデータ配信システムにおいても、多種多様、かつ、相当数のコンテンツデータを記憶する大容量データ記憶装置が望まれる。

20 この場合、大容量のデータ記憶装置において相当数のライセンスを記憶できるデータ記憶部が必要とされる。そして、上述したデータ配信システムにおいてライセンスの送受信処理が中断したとき、その中断した送受信中のライセンスが記憶されているか否かを確認するために、相当数のライセンスを記憶することができるライセンス記憶部内を検索することは、記憶できるライセンスの数が増える

25 ほど、その検索に時間がかかることになる。

従来のシステムにおいては、このような場合、全てのライセンス記憶部を逐一検索して特定するしかなく、検索に要する処理時間が問題とされていた。

発明の開示

そこで、この発明は、かかる課題を解決するためになされたものであり、その目的は、相当数のライセンスを記憶できるライセンス記憶部の中から送受信処理中のライセンスの記憶状態を迅速に確認でき、特にライセンスの送受信処理が中断したときに、ライセンスの保護と再処理の高速化とを両立するデータ記憶装置を提供することである。

そして、さらに、この発明は、ライセンスに限られず同様の保護が必要とされる機密データ全般に対して適用できるデータ記憶装置を提供することを目的とする。

この発明によれば、データ記憶装置は、機密データを保護するための所定の入出力手順に従って機密データの入出力を行ない、かつ、機密データを記憶するデータ記憶装置であって、外部とデータのやり取りを行なうインターフェース部と、機密データを記憶する第1の記憶部と、所定の入出力手順に従った機密データの入出力に関するログ情報と入出力の対象となる機密データの第1の記憶部における記憶位置を示すアドレスとを記憶する第2の記憶部とを備える。

好ましくは、データ記憶装置は、機密データの入出力を制御する制御部をさらに備え、ログ情報は、入出力の対象となる機密データを識別する識別コードと、入出力の対象となる機密データの第1の記憶部における記憶状態を示す第1のステータスとを含み、制御部は、所定の入出力手順に従って、入出力の対象となる機密データの識別コードとアドレスとをインターフェース部を介して受取ると第2の記憶部に記憶し、インターフェース部を介して受ける外部からの要求に応じて、第2の記憶部に記憶された識別コードとアドレスとに基づいて第1の記憶部における機密データの記憶状態を確認し、記憶状態に基づいて第1のステータスを更新する。

好ましくは、ログ情報は、入出力の対象となった機密データの入出力における所定の入出力手順の進行状態を記録する第2のステータスをさらに含み、制御部は、所定の入出力手順の進行に応じて第2のステータスを更新する。

好ましくは、ログ情報は、所定の入出力手順を特定する手順特定情報をさらに含み、制御部は、手順特定情報を新たに取得するごとに手順特定情報を更新する。

好ましくは、データ記憶装置は、所定の入出力手順に従って、インターフェー

ス部を介して機密データの提供元または提供先との間に暗号通信路を確立し、確立された暗号通信路を用いて機密データの受信または送信を行なう暗号通信部をさらに備え、所定の入出力手順の1つであって、機密データを受信して記憶する入力手順において、暗号通信部は、入力手順に従って機密データを受信し、制御部は、インターフェース部を介してアドレスを受取ると第2の記憶部に受取ったアドレスを記憶し、受取ったアドレスによって特定される第1の記憶部上の記憶位置に暗号通信部が受信した機密データを記憶する。

好ましくは、入力手順において、暗号通信部は、第1のセッション鍵を生成し、制御部は、暗号通信部によって第1のセッション鍵が生成されるごとに、第1のセッション鍵によって手順特定情報を更新する。

好ましくは、データ記憶装置は、ログ情報またはログ情報の一部に対して電子署名を施した署名付きログ情報を生成する署名部をさらに備え、所定の入出力手順の1つであって、入力手順が中断した場合にその中断した入力手順を復元する再入力手順において、制御部は、第2の記憶部に記憶されたログ情報に含まれる第1のステータスを更新し、ログ情報を第2の記憶部から取得して署名部に与え、署名部は、更新された第1のステータスが含まれるログ情報を受取って署名付きログ情報を生成し、暗号通信部は、再入力手順に従って、署名部によって生成された署名付きログ情報を確立された暗号通信路を用いて送信する。

好ましくは、所定の入出力手順の1つであって、第1の記憶部に記憶された機密データを外部へ出力する出力手順において、制御部は、インターフェース部を介してアドレスを受取ると第2の記憶部に受取ったアドレスを記憶し、受取ったアドレスによって特定される第1の記憶部上の記憶位置から機密データを取得して暗号通信部へ与え、暗号通信部は、出力手順に従って、制御部から与えられた機密データを送信する。

好ましくは、出力手順において、暗号通信部は、外部で生成された第2のセッション鍵を受信し、制御部は、暗号通信部が第2のセッション鍵を受信するごとに、受信した第2のセッション鍵によって手順特定情報を更新する。

好ましくは、データ記憶装置は、外部から受信した署名付きログ情報の正当性を検証して認証するログ認証部をさらに備え、所定の入出力手順の1つであって、

出力手順が中断した場合にその中断した出力手順を復元する再出力手順において、暗号通信部は、再出力手順に従って、署名付きログ情報を受信してログ認証部を与え、ログ認証部は、暗号通信部から受信した署名付きログ情報を検証し、制御部は、受信した署名付きログ情報が正当であると認証されたとき、第2の記憶部に記憶されたログ情報と受信した署名付きログ情報とに基づいて出力手順が中断したか否かを判断し、出力手順が中断したと判断したとき、第2の記憶部に記憶されたアドレスによって特定される第1の記憶部上の記憶位置を出力手順が中断する前の記憶状態に復元可能か否かを判断し、復元可能と判断したとき、出力手順が中断する前の記憶状態に記憶位置を復元し、中断された出力手順を再開する。

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御部は、第1の記憶部における機密データの記憶状態を確認するとき、アドレスによって特定される第1の記憶部上の記憶位置に記憶されている機密データに含まれる識別コードによって機密データを特定する。

好ましくは、所定の入出力手順の1つであって、機密データをインターフェース部を介して受取って第1の記憶部に記憶する入力手順において、制御部は、受取った機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データを第1の記憶部に記憶することなく、入力手順を中止する。

好ましくは、所定の入出力手順の1つであって、第1の記憶部に記憶された機密データをインターフェース部を介して出力する出力手順において、制御部は、アドレスによって特定される第1の記憶部上の記憶位置に記憶されている機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データの出力を行なうことなく、出力手順を中止する。

好ましくは、データ記憶装置は、ログ情報に対する署名データを生成し、生成した署名データをログ情報に添付した署名付きログ情報を生成する署名部をさらに備え、機密データをインターフェース部を介して受取って第1の記憶部に記憶する入力手順が中断した場合、中断した入力手順を再開する再入力手順において、制御部は、署名部によって生成された署名付きログ情報をインターフェース部を介して出力する。

好ましくは、データ記憶装置は、インターフェース部を介して機密データの提供先から受取った、提供先のもう1つのログ情報に対する署名データがもう1つのログ情報に添付されたもう1つの署名付きログ情報の正当性を検証して認証するログ認証部をさらに備え、第1の記憶部に記憶された機密データをインターフェース部を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証部は、中断した出力手順における機密データの提供先から受取ったもう1つの署名付きログ情報の正当性を検証し、制御部は、もう1つの署名付きログ情報が正当でないと認証されたとき、または、もう1つの署名付きログ情報が正当であると認証され、かつ、もう1つの署名付きログ情報と第2の記憶部に記憶されるログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

好ましくは、機密データは、暗号化されたコンテンツデータを復号して利用するための復号鍵であって、暗号化されたコンテンツデータを記憶するための第3の記憶部をさらに備える。

図面の簡単な説明

図1は、データ配信システムを概念的に説明する概略図である。

図2は、図1に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を示す図である。

図4は、図1に示すライセンス提供装置の構成を示す概略ブロック図である。

図5は、図1に示す端末装置の構成を示す概略ブロック図である。

図6は、図1に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

図7は、図6に示すハードディスクにおけるセキュアデータ記憶部のメモリ構成を示す図である。

図8は、図1に示すデータ配信システムにおける配信処理を説明するための第1のフローチャートである。

図 9 は、図 1 に示すデータ配信システムにおける配信処理を説明するための第 2 のフローチャートである。

図 10 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第 1 のフローチャートである。

5 図 11 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第 2 のフローチャートである。

図 12 は、図 1 に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第 3 のフローチャートである。

10 図 13 は、複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

図 14 は、図 13 に示すシステムにおける複製または移動処理を説明するための第 1 のフローチャートである。

図 15 は、図 13 に示すシステムにおける複製または移動処理を説明するための第 2 のフローチャートである。

15 図 16 は、図 13 に示すシステムにおける複製または移動処理中の再書込処理を説明するための第 1 のフローチャートである。

図 17 は、図 13 に示すシステムにおける複製または移動処理中の再書込処理を説明するための第 2 のフローチャートである。

20 図 18 は、図 13 に示すシステムにおける複製または移動処理中の再書込処理を説明するための第 3 のフローチャートである。

図 19 は、図 5 に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

発明を実施するための最良の形態

25 以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

図 1 は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

なお、以下では、デジタル放送網により配信された映像データを端末装置 10 により受信して端末装置 10 に装着されたデータ記憶装置である HD (ハードディスク) 20 に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク 30 に接続される端末装置 10 によりネットワーク 30 を介してライセンス提供装置 40 から受信して HD 20 に格納し、暗号化された映像データを端末装置 10 に内蔵された専用の再生回路 (図示せず) にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモリカードなどにおいても適用することが可能である。

図 1 を参照して、端末装置 10 は、デジタル放送網により配信される、暗号化された映像データ (以下、コンテンツデータとも呼ぶ) をアンテナ 11 を介して受信し、HD 20 に記憶する。暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むライセンスを管理し配信するライセンス提供装置 40 は、ライセンスの配信を求めてアクセスしてきた端末装置 10 に装着された HD 20 が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、HD 20 が正当なデータ記憶装置であった場合のみ、端末装置 10 に対して HD 20 においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置 10 は、ネットワーク 30 に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着された HD 20 へ送信する。

図 1 においては、たとえば、HD 20 は、端末装置 10 に着脱可能な構成となっている。端末装置 10 に装着された HD 20 は、端末装置 10 により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえで HD 20 内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコ

コンテンツ鍵と暗号化コンテンツデータとを端末装置 10 に与える。

そして、端末装置 10 のユーザは、端末装置 10 においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

このような構成とすることで、端末装置 10 のユーザは、ライセンス管理機能を備え、正規な認証データを有する HD 20 を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、コンテンツのライセンスを管理するライセンス提供装置 40 であってもよいし、インターネットなどのデジタル通信網を介して接続されるライセンス提供装置 40 とは別の配信サーバであってもよく、また、他のユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

したがって、本発明の実施の形態においては、HD 20、端末装置 10 およびライセンス提供装置 40 のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理の中断によるライセンスの消失を防ぎ、かつ、ライセンスが重複して存在することがないシステムの構成について説明する。

図 2 は、図 1 に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

データ D_c は、コンテンツデータであって、ここでは映像データである。データ D_c は、コンテンツ鍵 K_c で復号可能な暗号化が施され、暗号化コンテンツデータ E (K_c, D_c) の形式でデジタル放送網により端末装置 10 のユーザに配布される。

なお、以下においては、E (X, Y) という表記は、データ Y を、復号鍵 X に

より復号可能な暗号化を施したことを示すものとする。また、データD_cに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報D_iが配布される。

また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスID (LID) が端末装置10を介してライセンス提供装置40とHD20との間でやり取りされる。さらに、ライセンスとしては、データD_cおよびコンテンツ鍵K_cを識別するためのコードであるデータID

(DID) や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ACが存在する。

コンテンツ鍵K_cと、制御情報ACと、DIDと、LIDとを併せて、以後、ライセンスLICと総称することとする。DIDは、データD_cとコンテンツ鍵K_cとの対に対して割り当てられた識別情報、すなわち、暗号化データE (K_c, D_c) を識別するための識別情報となる。DIDは、ライセンスLICの他に、暗号化データE (K_c, D_c) とともに常に扱われる付加情報D_iにも含まれ、参照できるようになっている。

図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

HD20などのデータ記憶装置および端末装置10などに備えられる再生回路には、固有のクラス公開鍵K_{PCmy}およびK_{PCpy}がそれぞれ設けられ、クラス公開鍵K_{PCmy}およびK_{PCpy}は、データ記憶装置に固有のクラス秘密鍵K_{cm y}および再生回路に固有のクラス秘密鍵K_{c p y}によってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「y」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

また、データ記憶装置のクラス証明書としてC_{my}が設けられ、再生回路のクラス証明書としてC_{p y}が設けられる。これらのクラス証明書は、データ記憶装

置および再生回路のクラスごとに異なる情報を有する。

データ記憶装置のクラス証明書 C_{my} は、 $KP_{cmy} // I_{cmy} // E(K_a, H(KP_{cmy} // I_{cmy}))$ の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書 C_{py} は、 $KP_{cpy} // I_{cpy} // E(K_a, H(KP_{cpy} // I_{cpy}))$ の形式で出荷時に再生回路に記憶される。ここで、 $X // Y$ は、 X と Y との連結を表わし、 $H(X)$ は、ハッシュ関数により演算されたデータ X のハッシュ値を表わす。マスター鍵 K_a は、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局（図示せず）によって安全に管理運用される。また、クラス情報 I_{cmy} 、 I_{cpy} は、クラスごとの機器に関する情報およびクラス公開鍵を含む情報データである。

また、 $E(K_a, H(KP_{cmy} // I_{cmy}))$ および $E(K_a, H(KP_{cpy} // I_{cpy}))$ は、それぞれ $KP_{cmy} // I_{cmy}$ および $KP_{cpy} // I_{cpy}$ に対する電子署名を行なった署名データである。

なお、認証局は、署名データを作成する公的な第三者機関であり、署名データ $E(K_a, H(KP_{cmy} // I_{cmy}))$ および $E(K_a, H(KP_{cpy} // I_{cpy}))$ は、認証局によって生成される。

認証鍵 KPa は、クラス証明書を検証するための鍵であり、マスター鍵 K_a と対をなす公開鍵である。

さらに、データ記憶装置に対して安全かつ確実にライセンス LIC を送信するための鍵として、データ記憶装置という媒体ごとに管理される個別公開鍵 KP_{omz} と、個別公開鍵 KP_{omz} で暗号化されたデータを復号することが可能な個別秘密鍵 K_{omz} とが存在する。ここで、記号「 z 」は、データ記憶装置を個別に識別するための識別子である。

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置 40、データ記憶装置（HD 20）、および端末装置 10 の再生回路において生成されるセッション鍵 $Ks1x$ 、 $Ks2x$ が用いられる。

ここで、セッション鍵 $Ks1x$ 、 $Ks2x$ は、ライセンス提供装置 40、データ記憶装置（HD 20）、もしくは端末装置 10 の再生回路間の通信の単位ある

いはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。

「セッション」には、ライセンス提供装置 40 からデータ記憶装置 (HD 20) へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置 (HD 20) から端末装置 10 の再生回路へライセンスを出力する「再生許諾セッション」がある。

これらのセッション鍵 K_{s1x} 、 K_{s2x} は、各セッションごとに固有の値を有することにより、ライセンス提供装置 40、データ記憶装置 (HD 20)、および端末装置 10 の再生回路によって管理される。具体的には、セッション鍵 K_{s1x} は、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵 K_{s2x} は、ライセンスの受信側によってセッションごとに発生される。なお、記号「x」は、セッションにおける一連の処理を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンス LIC、またはコンテンツ鍵を含むライセンス LIC の一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

図 4 は、図 1 に示したライセンス提供装置 40 の構成を示す概略ブロック図である。

ライセンス提供装置 40 は、管理対象のライセンスを保持するデータベースであるコンテンツ DB 402 と、ライセンスを配信する配信セッションにおける一切の通信記録を記憶保持するデータベースであるログ DB 404 と、コンテンツ DB 402 およびログ DB 404 とバス BS1 を介してデータをやり取りし、所定の処理を行なうためのデータ処理部 410 と、ネットワーク 30 を介して端末装置 10 とデータ処理部 410 との間でデータ授受を行なうための通信装置 450 とを備える。

データ処理部 410 は、バス BS1 上のデータに応じて、データ処理部 410 の動作を制御するための配信制御部 412 と、配信制御部 412 により制御されて、配信セッション時にセッション鍵 K_{s1x} を発生するためのセッション鍵発

生部 4 1 4 と、認証鍵 KPa を保持する KPa 保持部 4 1 6 と、データ記憶装置のクラス証明書 Cmy を通信装置 4 5 0 およびバス $BS1$ を介して受け、 KPa 保持部 4 1 6 から受ける認証鍵 KPa によって行なわれる、クラス証明書 Cmy の後半部である署名データ $E(Ka, H(KPcmy // Icm y))$ の復号処理と、クラス証明書 Cmy の前半部である $KPcmy // Icm y$ のハッシュ値の計算とを行ない、両者の結果を比較チェックしてクラス証明書 Cmy の検証を行なう認証部 4 1 8 と、セッション鍵発生部 4 1 4 により生成されたセッション鍵 $Ks1x$ を認証部 4 1 8 によってクラス証明書 Cmy から抽出したクラス公開鍵 $KPcmy$ を用いて暗号化する暗号処理部 4 2 0 と、セッション鍵 $Ks1x$ によって暗号化されたデータを復号する復号処理部 4 2 2 とを含む。

データ処理部 4 1 0 は、さらに、配信制御部 4 1 2 から与えられるライセンス LIC を、復号処理部 4 2 2 から与えられたデータ記憶装置の個別公開鍵 $KPomz$ によって暗号化する暗号処理部 4 2 4 と、暗号処理部 4 2 4 の出力を、復号処理部 4 2 2 から与えられた、データ記憶装置が発生したセッション鍵 $Ks2x$ によってさらに暗号化する暗号処理部 4 2 6 とを含む。

なお、個別公開鍵 $KPomz$ およびセッション鍵 $Ks2x$ は、セッション鍵 $Ks1x$ によって暗号化されたうえで提供される。復号処理部 4 2 2 は、これを復号して個別公開鍵 $KPomz$ およびセッション鍵 $Ks2x$ を得る。

ライセンス提供装置 4 0 の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図 5 は、図 1 に示した端末装置 1 0 の構成を説明するための概略ブロック図である。

端末装置 1 0 は、デジタル放送網によって伝送される信号を受信するアンテナ 1 0 2 と、アンテナ 1 0 2 からの信号を受けてベースバンド信号に変換、あるいはアンテナ 1 0 2 から送信するデータを変調してアンテナ 1 0 2 に与える受信部 1 0 4 と、端末装置 1 0 をネットワーク 3 0 に接続するモデム 1 0 6 と、端末装置 1 0 の各部のデータ授受を行なうバス $BS2$ と、バス $BS2$ を介して端末装置 1 0 の動作を制御するコントローラ 1 0 8 と、HD 2 0 とバス $BS2$ との間のデータの授受を制御する HD インタフェース部 1 1 0 と、HD 2 0 に記憶された暗

号化コンテンツデータおよびライセンスによってコンテンツデータの再生を行なう再生回路150とを含む。

再生回路150は、上述したクラス証明書 Cp_y を保持する認証データ保持部1502を含む。ここで、再生回路150のクラス y は、 $y=3$ であるとする。

- 5 再生回路150は、さらに、クラス固有の復号鍵であるクラス秘密鍵 K_{cp3} を保持する K_{cp} 保持部1504と、クラス秘密鍵 K_{cp3} によって復号する復号処理部1506と、再生許諾セッションにおいて、セッション鍵 K_{s2x} を乱数等により発生するセッション鍵発生部1508と、セッション鍵発生部1508が発生したセッション鍵 K_{s2x} をHD20で発生したセッション鍵 K_{s1x} によって暗号化する暗号処理部1510と、セッション鍵 K_{s2x} によって暗号化されたコンテンツ鍵 K_c をセッション鍵 K_{s2x} によって復号する復号処理部1512と、バスBS2より暗号化コンテンツデータ $E(K_c, D_c)$ を受けて、復号処理部1512からのコンテンツ鍵 K_c によって暗号化コンテンツデータ $E(K_c, D_c)$ を復号してデータ D_c を再生部1516へ出力する復号処理部1514と、復号処理部1514から出力されたコンテンツデータ D_c を受けてそれを再生する再生部1516と、再生部1516の出力をデジタル信号からアナログ信号に変換するDA変換部1518と、DA変換部1518の出力をテレビモニターなどの外部出力装置（図示省略）へ出力するための端子1520とを含む。

- 20 なお、再生回路150は、セキュリティを向上させるために1チップ構成の半導体デバイスであることが好ましい。さらには、再生回路150は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

端末装置10の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

- 25 図6は、図1に示すHD20の構成を説明するための概略ブロック図である。

すでに説明したように、ハードディスクのクラス公開鍵およびクラス秘密鍵として、 K_{Pcmy} および K_{cmy} が設けられ、ハードディスクのクラス証明書 C_{my} が設けられるが、HD20においては、自然数 $y=1$ で表わされるものとする。また、HD20を識別する自然数 z は $z=2$ で表されるものとする。

図6を参照して、HD20は、暗号通信部268と、セキュアデータ記憶部250と、ノーマルデータ記憶部270と、端子210と、ATA (A T - A t t a c h m e n t) インタフェース部212と、コントローラ214とを含む。

5 端子210は、HD20を端末装置10のHDインターフェース110と物理的および電氣的に接続する。ATAインタフェース部212は、端末装置10のHDインターフェース部110と端子210を介して信号を授受する。バスBS3は、HD20におけるデータ伝送路である。

10 暗号通信部268は、クラス証明書Cm1として認証データKPcm1//Icm1//E(Ka, H(KPcm1//Icm1))を保持する認証データ保持部202と、クラス秘密鍵Kcm1を保持するKcm保持部204と、個別秘密鍵Kom2を保持するKom保持部206と、個別秘密鍵Kom2によって復号可能な個別公開鍵KPopm2を保持するKPopm保持部208とを含む。

15 このように、ハードディスクドライブというデータ記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をハードディスクドライブ単位で実行することが可能になる。

20 暗号通信部268は、さらに、Kom保持部206により与えられた個別秘密鍵Kom2により復号する復号処理部216と、KPa保持部218から認証鍵KPaを受け、バスBS3に出力されたデータの認証鍵KPaによる復号処理を実行して復号結果をコントローラ214へ出力し、かつ、得られたクラス公開鍵KPcm1を暗号処理部222へ出力する認証部220と、切換スイッチ260によって選択的に与えられるセッション鍵Ks1xまたはKs2xによって、切換スイッチ262によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号処理部224とを含む。

25 暗号通信部268は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵Ks1x, Ks2xを発生するセッション鍵発生部226と、セッション鍵発生部226の出力したセッション鍵Ks1xを認証部220によって得られるクラス公開鍵KPCpyあるいはKPCmyによって暗号化する暗号処理部222と、セッション鍵発生部226が発生したセッション

鍵 K_{s1x} または K_{s2x} によって暗号化されたデータを受けてセッション鍵 K_{s1x} または K_{s2x} によって復号する復号処理部228とを含む。

暗号通信部268は、さらに、クラス公開鍵 K_{Pcm1} によって暗号化されたデータを受けてクラス秘密鍵 K_{cm1} によって復号する復号処理部230と、
5 ライセンスLICをHD20からHD21へ移動または複製する際に、提供先のHD21から受信した個別公開鍵 K_{Pomz} ($z \neq 2$) によりライセンスLICを暗号化する暗号処理部232とを含む。

セキュアデータ記憶部250は、ライセンスLICと、HD20が処理しているセッションの処理記録であるログとを記憶する。そして、ライセンスLICは、
10 セキュアデータ記憶部250内のライセンスメモリ250Aに格納され、ログは、セキュアデータ記憶部250内のログメモリ250Bに格納される。セキュアデータ記憶部250は、たとえば半導体メモリによって構成され、外部から直接アクセスすることができない構造を有する記憶領域である。

図7は、セキュアデータ記憶部250におけるメモリ構成を示した図である。

図7を参照して、ライセンスメモリ250Aは、HD20が複数のコンテンツデータを記憶可能であることに対応して、ライセンスLIC（コンテンツ鍵 K_c 、
15 制御情報AC、ライセンスID（LID）、データID（DID））を複数格納することができる構成になっている。

そして、HD20においては、ライセンスメモリ250Aに格納されたライセンスLICは、セキュアデータ記憶部250における格納アドレス（以下、LBA;
20 $Logical\ Block\ Address$ と称する。）により管理される。そして、各セッションにおいて記憶あるいは出力されるライセンスLICは、全てLBAにより特定される。

また、セキュアデータ記憶部250には、有効フラグメモリ250Cが設けら
25 れる。有効フラグメモリ250Cは、ライセンスメモリ250A上の記憶位置を特定するLBAそれぞれに対応して設けられ、対応するLBAによって特定される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

有効フラグメモリ250Cのフラグが「有効」であるとき、フラグに対応するLBAによって特定されるライセンスメモリ250A上の記憶位置に記憶されて

いるライセンスLICは利用可能であり、ユーザはそのライセンスLICに対応したコンテンツデータを再生したり、そのライセンスLICの移動・複製を行なうことができる。

一方、有効フラグメモリ250Cのフラグが「無効」であるとき、そのフラグ
5 に対応するLBAによって特定されるライセンスメモリ250A上の記憶位置に
記憶されているライセンスLICは利用不可であり、HD20のコントローラ2
14によって、そのLBAからのライセンスLICは拒否される。すなわち、消
去されたのと同じ状態である。したがって、ユーザはそのライセンスLICに対
10 応したコンテンツデータを再生することはできない。この有効フラグメモリ25
0Cのフラグは、ライセンスの新たな記憶によって「有効」とされ、ライセンス
の移動によって「無効」とされる。

ログメモリ250Bには、セッションの対象となるライセンスLICを特定す
るライセンスID(LID)を格納するライセンスID領域2501、セッション
15 においてライセンスLICの受信側のデータ記憶装置によって生成されたセッ
ション鍵Ks2xを格納するKs2x領域2502、動作中のセッションにおける
処理の状態を示すステータスST1を格納するST1領域2503およびライ
センスID領域2501に格納されるライセンスIDに対応したライセンスの記
憶状態を示すステータスST2を格納するST2領域2504、ライセンスを移
20 動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデー
タ記憶装置のクラス公開鍵KPCmxを格納するKPCmx領域2505、並び
に当該セッションにおいてライセンスLICを出力あるいは記憶するために指示
されたLBAを格納するLBA領域2506が設けられ、一連のセッションの処
理が進行するにつれて、上記各領域のデータが更新あるいは参照されていく。ス
テータスST1は、「受信待」、「受信済」、「送信待」および「送信済」の4
25 状態のいずれかであり、ステータスST2は、「データ有」、「データ無」およ
び「移動済」の3状態のいずれかである。

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、
そのセッションにおいて送受信されていたライセンスLICに対して、ログメモ
リ250B内のLID領域2501に格納されているライセンスIDと、LBA

領域 2506 に格納された LBA とによって当該ライセンス LIC の記憶状態が確認され、その確認結果に応じてステータス ST2 が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ 250B 内に格納されているライセンス LIC、セッション鍵 Ks2x、ステータス ST1 およびステータス ST2 を受取って、自身が記録するログの内容と受取ったライセンス LIC、セッション鍵 Ks2x、ステータス ST1 およびステータス ST2 とを確認することにより、再度のライセンスの送受信を行なってもよいか否かの判断がされる。

なお、セッション鍵 Ks2x は、各セッションを特定するために記憶され、セッション鍵 Ks2x を共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

このような構成とすることにより、特に、相当数のライセンスが格納できるライセンスメモリ 250A を有する HD20 において、あるセッションにおける処理の中断が発生したときなどライセンスメモリ 250A におけるライセンスの記憶状態を確認する必要があるときに（あるいはライセンスの有無を特定）、容易に確認を行ない、ステータス ST2 を更新できる。

なお、以下、再送信の確認時においてライセンスの受信側となった場合に、ライセンスの送信側に対して出力するログメモリ 250B に格納されたライセンス ID (LID)、セッション鍵 Ks2x およびステータス ST1、ST2 は、出力ログと総称する。また、HD20 においてのみ参照されるログメモリ 250B に格納された受信側のクラス公開鍵 KPCmx および LBA は、内部ログと総称する。

また、ステータス ST2 には、出力ログが出力される際に、ログメモリ 250B に格納されているライセンス ID (LID) と LBA とによってライセンスメモリ 250A における対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

ここで、再び図 6 を参照して、ノーマルデータ記憶部 270 は、暗号化コンテンツデータを記憶する。ノーマルデータ記憶部 270 は、データが記憶される円

盤状の磁気記録媒体 2701 と、磁気記録媒体 2701 を回転させるモータ 2702 と、モータ 2702 を制御するサーボ制御部 2703 と、磁気記録媒体 2701 上における磁気ヘッドの位置を制御するシーク制御部 2704 と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部 2705 とを含む。ノーマルデータ記憶部 270 の構成は、一般の公知のハードディスクの構成と変わる
5 ところはなく、詳細な説明は省略する。

コントローラ 214 は、さらに、ATA インターフェース部 212 を介して外部との間でデータ授受、制御情報 AC に基づくライセンスの出力に関する判断、およびセキュアデータ記憶部 250 の管理などの HD 20 内の動作を制御する。

10 なお、コントローラ 214、暗号通信部 268 およびセキュアデータ記憶部 250 は、耐タンパモジュール領域に構成される。

以下、図 1 に示すデータ配信システムにおける各セッションの動作について説明する。

〔配信〕

15 まず、図 1 に示すデータ配信システムにおいて、ライセンス提供装置 40 から端末装置 10 に装着された HD 20 へライセンスを配信する動作について説明する。

図 8 および図 9 は、図 1 に示すデータ配信システムにおいて、端末装置 10 のユーザが端末装置 10 から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンス提供装置 40 から端末装置 10 に装着された
20 HD 20 へライセンスの配信が行なわれる際の処理（配信セッション）を説明するための第 1 および第 2 のフローチャートである。

図 8 における処理開始以前に、端末装置 10 のユーザは、端末装置 10 をモデム 106 によりネットワーク 30 に接続し、端末装置 10 をネットワーク 30 を
25 介してライセンス提供装置 40 に接続していることを前提としている。

図 8 を参照して、端末装置 10 のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置 10 のコントローラ 108 は、バス BS 2 および HD インターフェース部 110 を介して HD 20 へクラス証明書の出力要求を出力する（ステップ S1）。HD 20 のコントローラ 214

は、端子210およびATAインタフェース部212を介してクラス証明書の出力要求を受理すると（ステップS2）、バスBS3を介して認証データ保持部202からクラス証明書 $Cm1 = KP_{cm1} // I_{cm1} // E(Ka, H(KP_{cm1} // I_{cm1}))$ を読み出し、クラス証明書 $Cm1$ をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS3）。

端末装置10のコントローラ108は、HD20からHDインターフェース部110およびバスBS2を介してクラス証明書 $Cm1$ を受理すると（ステップS4）、受理したクラス証明書 $Cm1$ をモデム106およびネットワーク30を介してライセンス提供装置40へ送信する（ステップS5）。

ライセンス提供装置40では、端末装置10からクラス証明書 $Cm1$ を受信すると（ステップS6）、受信した $Cm1$ が正当なクラス証明書であるか否かを検証する（ステップS7）。検証処理は次のように行なわれる。

ライセンス提供装置40は、クラス証明書 $Cm1 = KP_{cm1} // I_{cm1} // E(Ka, H(KP_{cm1} // I_{cm1}))$ を受理すると、HD20から出力されたクラス証明書 $Cm1$ に含まれる署名データ $E(Ka, H(KP_{cm1} // I_{cm1}))$ を認証部418において認証鍵 KPa で復号する。そして、さらに、認証部418は、クラス証明書 $Cm1$ に含まれる $KP_{cm1} // I_{cm1}$ のハッシュ値を演算し、認証鍵 KPa で復号した $H(KP_{cm1} // I_{cm1})$ の値と比較する。配信制御部412は、認証部418における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、HD20から受理したクラス証明書 $Cm1$ は、正当な証明書であると判断する。

ステップS7において、クラス証明書 $Cm1$ が正当な証明書であると判断された場合、配信制御部418は、クラス証明書 $Cm1$ を承認し、クラス公開鍵 KP_{cm1} を受理する（ステップS8）。そして、次の処理（ステップS9）へ移行する。正当なクラス証明書でない場合には、配信制御部412はクラス証明書 $Cm1$ を非承認とし、クラス証明書 $Cm1$ を受理しないでエラー通知を端末装置10へ出力し（図9のステップS44）、端末装置10においてエラー通知が受理されると（図9のステップS45）、配信セッションが終了する。

認証の結果、ライセンス提供装置40において、正当なクラス証明書を持つハ

ードディスクを装着した端末装置からのアクセスであることが確認され、ステップS 8においてクラス公開鍵K P c m 1が受理されると、配信制御部4 1 2は、ライセンスID (L I D) を生成し (ステップS 9)、さらに制御情報A Cを生成する (ステップS 1 0)。そして、セッション鍵発生部4 1 4は、配信のため
5 のセッション鍵K s 1 aを生成する (ステップS 1 1)。セッション鍵K s 1 aは、認証部4 1 8によって得られたHD 2 0に対応するクラス公開鍵K P c m 1によって、暗号処理部4 2 0によって暗号化され、暗号データE (K P c m 1, K s 1 a) が生成される (ステップS 1 2)。

そして、配信制御部4 1 2は、ライセンスID (L I D) および暗号化された
10 セッション鍵K s 1 aを1つのデータ列L I D//E (K P c m 1, K s 1 a)として、バスB S 1および通信装置4 5 0を介して外部に出力する (ステップS 1 3)。

端末装置1 0は、ネットワーク3 0を介してL I D//E (K P c m 1, K s 1 a)を受信すると (ステップS 1 4)、受信したL I D//E (K P c m 1, K s 1 a)をHD 2 0へ出力する (ステップS 1 5)。そして、HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介してL I D//E (K P c m 1, K s 1 a)を受理する (ステップS 1 6)。コントローラ2 1 4は、バスB S 3を介して受理したE (K P c m 1, K s 1 a)を復号処理部2 3 0へ与え、復号処理部2 3 0は、K c m保持部2 0 4に保持されるH
15 D 2 0に固有なクラス秘密鍵K c m 1によって復号処理することにより、セッション鍵K s 1 aを復号し、セッション鍵K s 1 aを受理する (ステップS 1 7)。

HD 2 0のコントローラ2 1 4は、ライセンス提供装置4 0で生成されたセッション鍵K s 1 aの受理を確認すると、ATAインターフェース部2 1 2および端子2 1 0を介してその旨を端末装置1 0に通知する。端末装置1 0のコントローラ1 0 8は、HDインターフェース部1 1 0およびバスB S 2を介して、HD
20 2 0においてセッション鍵K s 1 aが受理された旨の通知を受理すると、HD 2 0において配信動作時に生成されるセッション鍵の生成の要求通知をバスB S 2およびHDインターフェース部1 1 0を介してHD 2 0へ出力する (ステップS 1 8)。HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAコントロー

ラ 2 1 2 を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部 2 2 6 に対して HD 2 0 において配信動作時に生成されるセッション鍵 K_{s2a} の生成を指示する。そして、セッション鍵発生部 2 2 6 は、セッション鍵 K_{s2a} を生成する（ステップ S 1 9）。

- 5 セッション鍵発生部 2 2 6 は、セッション鍵 K_{s2a} を生成すると、バス BS 3 を介してコントローラ 2 1 4 へ出力し、セッション鍵 K_{s2a} を受けたコントローラ 2 1 4 は、ステップ S 1 6 において受理したライセンス ID (LID) とセッション鍵 K_{s2a} とをセキュアデータ記憶部 2 5 0 内のログメモリ 2 5 0 B へ格納するとともに、ステータス ST 1 を「受信待」にする（ステップ S 2 0）。
- 10 続いて、暗号処理部 2 2 4 は、切換スイッチ 2 6 0 の接点 P b を介して復号処理部 2 3 0 より与えられるセッション鍵 K_{s1a} によって、切換スイッチ 2 6 2 の接点 P d と P f とを順に切替えることによって与えられるセッション鍵 K_{s2a} と個別公開鍵 K_{Pom2} とからなる 1 つのデータ列を暗号化し、 $E(K_{s1a}, K_{s2a} // K_{Pom2})$ 生成する（ステップ S 2 1）。そして、暗号処理部 2 2 4 は、 $E(K_{s1a}, K_{s2a} // K_{Pom2})$ をバス BS 3 に出力する。バス BS 3 に出力された暗号化データ $E(K_{s1a}, K_{s2a} // K_{Pom2})$ は、コントローラ 2 1 4 により受理され、コントローラ 2 1 4 は、受理した暗号化データとライセンス ID (LID) とを 1 つのデータ列としたデータ $LID // E(K_{s1a}, K_{s2a} // K_{Pom2})$ を ATA インタフェース部 2 1 2 および
- 15 端子 2 1 0 を介して端末装置 1 0 へ出力する（ステップ S 2 2）。

そして、端末装置 1 0 は、データ $LID // E(K_{s1a}, K_{s2a} // K_{Pom2})$ を HD 2 0 から受理すると（ステップ S 2 3）、受理したデータをネットワーク 3 0 を介してライセンス提供装置 4 0 に出力する（ステップ S 2 4）。

- 25 ライセンス提供装置 4 0 は、データ $LID // E(K_{s1a}, K_{s2a} // K_{Pom2})$ を受信すると（ステップ S 2 5）、復号処理部 4 2 2 においてセッション鍵 K_{s1a} による復号処理を実行し、HD 2 0 で生成されたセッション鍵 K_{s2a} 、および HD 2 0 の個別公開鍵 K_{Pom2} を受理する（ステップ S 2 6）。
- 配信制御部 4 1 2 は、ライセンス ID (LID) に対応するデータ ID (DID) およびコンテンツ鍵 K_c をコンテンツ DB 4 0 2 から取得し（ステップ S 2

7)、ライセンスID (LID) および制御情報ACと併せた1つのデータ列としてのライセンスLIC=Kc//AC//DID//LIDを生成する。

配信制御部412は、生成したライセンスLICを暗号処理部424に与える。

暗号処理部424は、復号処理部422によって得られたHD20の個別公開鍵

5 KPom2によってライセンスLICを暗号化して暗号化データE (KPom2, LIC) を生成する (ステップS28)。そして、暗号処理部426は、暗号処理部424から受ける暗号化データE (KPom2, LIC) を、復号処理部422から受けるセッション鍵Ks2aによって暗号化し、暗号化データE (Ks2a, E (KPom2, LIC)) を生成する (ステップS29)。

10 図9を参照して、配信制御部412は、バスBS1および通信装置450を介して暗号化データE (Ks2a, E (KPom2, LIC)) を外部へ出力する (ステップS30)。端末装置10は、ネットワーク30を介して暗号化データE (Ks2a, E (KPom2, LIC)) を受取りすると (ステップS31)、受取った暗号化データをHD20へ出力する (ステップS32)。

15 HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE (Ks2a, E (KPom2, LIC)) を受取りすると (ステップS33)、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE (Ks2a, E (KPom2, LIC)) を復号し、HD20において、ライセンスLICが個別公開鍵KPom2により暗号化された暗号化ライセンスE (KPom2, LIC) が受取られる (ステップS34)。

20 そして、復号処理部228は、暗号化ライセンスE (KPom2, LIC) をバスBS3へ出力する。

コントローラ214の指示によって、暗号化ライセンスE (KPom2, LIC) は、復号処理部216において個別秘密鍵Kom2によって復号され、ライセンスLICが受取られる (ステップS35)。

25

HD20のコントローラ214は、ライセンスLICの受取を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部1

10 およびバスBS2を介して、HD20においてライセンスLICが受理された旨の通知を受理すると、HD20のセキュアデータ記憶部250において、その受信したライセンスLICを格納するLBAをバスBS2およびHDインターフェース110を介してHD20へ出力する（ステップS36）。HD20のコントローラ214は、端子210およびATAインターフェース部212を介してライセンスLICの格納先LBAを受理すると（ステップS37）、その受理したLBAをログメモリ250Bに記憶する（ステップS38）。

そして、コントローラ214は、受理したライセンスLICに含まれるライセンスID（LID）と、ステップS16において受理したライセンスLID（LID）とを比較し、一致しているか否かをチェックする（ステップS39）。コントローラ214は、LIDが一致しており、受理したライセンスLICが正しいものであると判断すると、端末装置10から受理したセキュアデータ記憶部250内のLBAに、受理したライセンスLICを記憶する（ステップS40）。

コントローラ214は、指定されたLBAにライセンスLICを記憶すると、有効フラグメモリ250CのそのLBAに対応するフラグを「有効」にする（ステップS41）。そして、コントローラ214は、さらに、ログメモリ250BのステータスST1を「受信済」にし（ステップS42）、配信セッションにおける一連の処理が終了したことを端末装置10に通知する。

そして、端末装置10において、HD20から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

一方、ステップS39において、コントローラ214は、LIDが一致せず、受理したライセンスLICが正しくないと判断すると、エラー通知を端末装置10へ出力し（ステップS43）、端末装置10は、エラー通知を受理すると（ステップS45）、処理を終了する。

図8および図9に示された配信処理においては、ライセンス提供装置40における処理履歴の記録に関する記載がなされていないが、図4に示すように、ライセンス提供装置40には、十分な記憶容量を持つログDB404が備えられており、配信セッションにおける各処理の進行に伴う処理履歴がログDB404に記憶される。また、ログDB404には、ライセンスの送信に伴う課金情報など

も記憶される。

図 8 および図 9 に示された配信処理における一連の処理において、ステップ S 2 5 からステップ S 4 4 の処理中に異常が発生して処理が中断したときは、再書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置 1 0 の電源が遮断されたり、ライセンス提供装置 4 0 側の異常、あるいは端末装置 1 0 とライセンス提供装置 4 0 との通信異常など、種々の異常ケースが考えられる。ここで、HD 2 0 内のログメモリ 2 5 0 B に格納されたステータス S T 2 を除く出力ログの内容がすべて格納されたステップ S 2 2 終了後からステップ S 4 4 までの処理中に処理が中断した場合には、HD 2 0 は、再書込処理を行なってライセンスの提供を受けることが可能である。ここでは、端末装置 1 0 の判断によって再書込処理を行なうものとしたため、端末装置 1 0 において処理の進行が確認できるステップ S 2 2 からステップ S 2 4 を除く、ステップ S 2 5 からステップ S 4 4 の処理中に処理が中断した場合を再書込処理の対象とし、他のステップにおける処理の中断においてはライセンス提供装置 4 0 からライセンスの提供がなされなかったものと判断し、図 8 および図 9 に示したフローチャートにしたがって、最初から処理を行なうこととした。

同様に、ライセンス提供装置 4 0 がライセンスを出力するまでのライセンス提供装置 4 0 内のステップ S 2 5 からステップ S 3 0 までの処理については、端末装置 1 0 において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図 8 および図 9 に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

図 1 0 から図 1 2 は、図 8 および図 9 において示した配信処理におけるステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したときに行なわれる再書込処理の第 1 から第 3 のフローチャートである。

図 1 0 を参照して、端末装置 1 0 は、ステップ S 2 5 からステップ S 4 4 の処理中に異常が発生したと判断すると、ライセンス L I C の再書込要求をネットワーク 3 0 を介してライセンス提供装置 4 0 へ出力する（ステップ S 1 0 1）。配信制御部 4 1 2 は、通信装置 4 5 0 およびバス B S 1 を介して再書込要求を受理すると（ステップ S 1 0 2）、セッション鍵発生部 4 1 4 にセッション鍵を生成

するように指示する。指示を受けたセッション鍵発生部414は、再書込処理のためのセッションキー鍵 K_{s1b} を生成する（ステップS103）。そして、配信制御部412は、このセッションにおいてHD20とやり取りしたログが格納されているログDB402からHD20に対応するクラス公開鍵 K_{Pcm1} を取得し（ステップS104）、暗号処理部420に与える。クラス公開鍵 K_{Pcm1} を受けた暗号処理部420は、クラス公開鍵 K_{Pcm1} をによりセッション鍵 K_{s1b} を暗号化し、 $E(K_{Pcm1}, K_{s1b})$ が生成される（ステップS105）。そして、配信制御部412は、 $E(K_{Pcm1}, K_{s1b})$ をバスBS1および通信装置450を介して外部に出力する（ステップS106）。

10 端末装置10は、ネットワーク30を介して $E(K_{Pcm1}, K_{s1b})$ を受理すると（ステップS107）、受理した $E(K_{Pcm1}, K_{s1b})$ をHD20へ出力する（ステップS108）。そして、HD20のコントローラ214は、端子210およびATAインタフェース部212を介して $E(K_{Pcm1}, K_{s1b})$ を受理する（ステップS109）。コントローラ214は、受理した E
15 (K_{Pcm1}, K_{s1b}) をバスBS3を介して復号処理部230へ与え、復号処理部230は、 K_{cm} 保持部204に保持されるHD20に固有なクラス秘密鍵 K_{cm1} によって復号処理することにより、セッション鍵 K_{s1b} を復号し、セッション鍵 K_{s1b} が受理される（ステップS110）。

HD20のコントローラ214は、ライセンス提供装置40で生成されたセッション鍵 K_{s1b} の受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10のコントローラ108は、HDインターフェース部110およびバスBS2を介して、HD20においてセッション鍵 K_{s1b} が受理された旨の通知を受理すると、セキュアデータ記憶部250に記憶されたログメモリ250Bの出力要求をバスBS2
20 およびHDインターフェース部110を介してHD20へ出力する（ステップS111）。

HD20のコントローラ214は、端子210およびATAコントローラ212を介してログメモリ250Bの出力要求通知を受理すると（ステップS112）、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICの

ライセンスID (LID) と、ログメモリ250Bに格納されたライセンスID (LID) とが一致するか否かをチェックする (ステップS113)。

コントローラ214は、両ライセンスID (LID) が一致すると判断すると、配信処理としては、ライセンス提供装置40からのライセンスLICの受理までは行なわれ、HD20においてライセンスLICは受理していると認識する。そうすると、コントローラ214は、ログメモリ250Bに格納されたLBAにより指示されるアドレスに記憶されるライセンスに対応する有効フラグメモリ250Cに格納されているフラグをチェックして、そのライセンスの有効性をチェックする (ステップS114)。

コントローラ214は、ライセンスが有効であると判断すると、ログメモリ250BのステータスST2を「データ有」に変更し、次の処理 (ステップS118) へ移行する。一方、コントローラ214は、ステップS114においてライセンスが無効であると判断すると、ログメモリ250BのステータスST2を「移動済」に変更し、次の処理 (ステップS118) へ移行する。

ステップ113において、コントローラ214は、比較したライセンスID (LID) が一致しないと判断したときは、ログメモリ250BのステータスST2を「データ無」に変更する (ステップS117)。

このように、ログメモリ250Bに格納されたLBAを用いて、そのLBAに記憶されるライセンスLICのライセンスID (LID) をLBAに基づいて直接確認できるので、ライセンスメモリ250Aに相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしに特定のライセンスID (LID) の有無などを判断することができる。

ステータスST2の変更処理がなされると、コントローラ214は、ログメモリ250BからライセンスID (LID)、ステータスST1、ST2およびセッション鍵Ks2cを取得する (ステップS118)。ここで、ログメモリ250Bに格納されているセッション鍵はKs2aであるが、表記の関係上、ログメモリ250Bから取得したセッション鍵をKs2cとしている。そして、コントローラ214は、取得したセッション鍵Ks2cをバスBS3を介して暗号処理部224へ出力する。

暗号処理部 224 は、切換スイッチ 260 の接点 P b を介して復号処理部 230 より与えられるセッション鍵 K_{s1b} によって、バス BS3 から取得したセッション鍵 K_{s2c} を暗号化し、 $E(K_{s1b}, K_{s2c})$ 生成する (ステップ S119)。そして、暗号処理部 224 は、生成した $E(K_{s1b}, K_{s2c})$ を

5 バス BS3 に出力する。バス BS3 に出力された $E(K_{s1b}, K_{s2c})$ は、コントローラ 214 により受理され、コントローラ 214 は、ステップ S118 において取得したデータとともに 1 つのデータ列 $LID//E(K_{s1b}, K_{s2c})//ST1//ST2$ を生成し、ハッシュ関数を用いてハッシュ値 $H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2)$ を生成する (ステップ S120)。そして、コントローラ 214 は、ハッシュ値 $H(LID//E$

10 $(K_{s1b}, K_{s2c})//ST1//ST2)$ をバス BS3 を介して暗号処理部 224 へ出力する。

暗号処理部 224 は、切換スイッチ 260 の接点 P b を介して復号処理部 230 より与えられるセッション鍵 K_{s1b} によって、バス BS3 から取得したハッシュ値 $H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2)$ を暗号

15 化し、 $E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ 生成する (ステップ S121)。そして、暗号処理部 224 は、生成した $E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ をバス BS3 に出力する。ここで、データ列 $LID//E(K_{s1b}, K_{s2c})//ST1//ST2$ を受信ログと称し、 $E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ は、受信ログに対してセッション鍵 K_{s1b} を用いて電子署名を行なった署名データである。また、ログメモリ 250B に格納されていたセッション鍵 K_{s2c} をセッション鍵 K_{s1b} を用いて暗号化するのは、セッション鍵 K_{s2c} の漏洩によるライセンスの流出の危険性を排除するためである。

25

コントローラ 214 は、バス BS3 から署名データを受理すると、ステップ S118 において取得した受信ログを用いて、署名付き受信ログ $LID//E(K_{s1b}, K_{s2c})//ST1//ST2//E(K_{s1b}, H(LID//E(K_{s1b}, K_{s2c})//ST1//ST2))$ を生成し、ATA インターフ

ェース部 212 および端子 210 を介して端末装置 10 へ出力する（ステップ S122）。

端末装置 10 は、署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を HD20 から受理すると（ステップ S123）、受理したデータをネットワーク 30 を介してライセンス提供装置 40 へ出力する

（ステップ S124）。そして、ライセンス提供装置 40 は、ネットワーク 30 を介して署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を受信する。（ステップ S125）

図 11 を参照して、ライセンス提供装置 40 は、受信した署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ の検証を行なう（ステップ S126）。検証処理は次のように行なわれる。

配信制御部 412 は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データ $E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を復号処理部 422 へ出力する。そして、復号処理部 422 は、ステップ S103 で生成したセッション鍵 $Ks1b$ によって署名データ $E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を復号する。一方、配信制御部 412 は、署名付き受信ログの前半部である受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2$ のハッシュ値を演算し、復号処理部 422 により復号された $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ の値と比較する。配信制御部 412 は、復号処理部 422 における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、HD20 から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置 40 において認証される。

ステップ S126 において HD20 から受理した署名付き受信ログが認証されると、配信制御部 412 は、受理したライセンス ID (LID) に基づいてログ DB404 を検索する（ステップ S127）。配信制御部 412 は、受理したラ

イセンスID (LID) がログDB404内に格納されており、HD20に対して確かに提供を行なったライセンスであると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS128)。

5 配信制御部412は、ステータスST1が「受信待」であり、ステータスST2が「データ無」であるとき、HD20に送信したはずのライセンスLICが何らかの異常によりHD20において受理されていないと判断し、受信したデータ列に含まれる暗号化データE (Ks1b, Ks2c) を復号処理部422へ出力してセッション鍵Ks1bによって復号し、セッション鍵Ks2cを受理する。そして、復号されたセッション鍵Ks2cは、バスBS1を介して配信制御部412へ出力され、配信制御部412においてセッション鍵Ks2cが受理される(ステップS129)。

15 そして、配信制御部412は、異常発生時のセッション鍵Ks2aを今回受理したセッション鍵Ks2cと比較チェックする(ステップS130)。配信制御部412は、セッション鍵Ks2aとセッション鍵Ks2cとが一致していると判断すると、ライセンスLICの再書込に対する許可通知を端末装置10へ出力する(ステップS133)。

一方、ステップS126においてHD20から受理したデータ列が認証されなかったとき、ステップS127においてHD20から受理したライセンスID (LID) がログDB404内に格納されておらず、HD20に対して提供を行なったライセンスであると判断できないとき、ステップS128において、HD20においてライセンスLICが受理されたものと判断されたとき、またはステップS130において、セッション鍵Ks2aがセッション鍵Ks2cと一致しないと判断されたときは、配信制御部412は、バスBS1および通信装置450を介してエラー通知を出力し(ステップS131)、端末装置10は、ネットワーク30を介してエラー通知を受理すると(ステップS132)、処理が終了する。すなわち、ライセンス提供装置40において、ライセンスの再書込が拒否されて処理が終了する。

25 端末装置10のコントローラ108は、ステップS133においてライセンス提供装置40が出力した許可通知を受理すると(ステップS134)、HD20

において配信動作時に生成されるセッション鍵の生成の要求通知をバスB S 2およびHDインターフェース部110を介してHD20へ出力する（ステップS135）。

HD20は、ライセンス提供装置40からの再書込処理許可通知に基づいて、
5 端末装置10からセッション鍵の生成要求通知を受理すると、以下、図8および図9において説明したステップS19から処理終了までの一連の処理において、セッション鍵K s 2 aに代えて新たなセッション鍵K s 2 bが生成され、そのセッション鍵K s 2 bが使用されるほかは、同様の処理が行なわれる。したがって、ステップS135に続く一連の処理の説明は繰返しになるので省略する。

10 なお、図10～図12のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップS101～S131、ステップS133およびステップS142～S160のいずれかのステップにおいて処理が中断した場合には、再び図10～図12のフローチャートにしたがって再書込処理を行なうことができる。一方、ステップS134～S141のいずれかのステップ
15 において処理が中断した場合には、図8および図9のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

このようにして、端末装置10に装着されたHD20が正規のクラス証明書C m 1を保持する機器であることを確認したうえで、クラス証明書C m 1に含まれて送信されたクラス公開鍵K P c m 1によってライセンス提供装置40およびHD20でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配
25 信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置であるHD20における受信ログをライセンス提供装置40へ送信することで、ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことが

できる。

その上、HD 20においてライセンスを記憶するLBAの指示がなされた場合において、そのLBAをログの一部として記録することによって、配信セッション中に異常が発生したとき、ログメモリ250Bに格納されたLBAにしたがって、そのセッションによって記録されるべきライセンスLICのライセンスメモリ250Aにおける記憶状態を、相当数のライセンスを記録できるライセンスメモリ250A内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、配信処理において迅速な再書込処理を行なうことができる。

- 10 なお、上記においては、署名付き受信ログは、 $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ としたが、検証の高速化を図るため、署名付き受信ログは、 $LID // ST1 // ST2 // H(Ks1b // LID // Ks2c // ST1 // ST2)$ としてもよい。この場合、署名付き受信ログの
- 15 検証によって、 $Ks1b$ および $Ks2c$ の共有が同時に確認されることとなる。また、署名時の2つの暗号化処理および検証時の2つの復号処理が省かれ、検証処理が高速化する。

[複製・移動]

- 図13は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図13を参照して、端末装置10にデータ記憶装置として2
- 20 台のハードディスクHD20、HD21が装着可能であり、端末装置10を介してHD20からHD21へライセンスの複製または移動が行なわれる。

- ここで、HD21は、HD20と異なるデータ記憶装置であるため、HD20とは異なる個別公開鍵 $KPom5$ と個別秘密鍵 $Kom5$ とを保持している。この
- 25 場合、HD21における識別子 z は、HD20の $z=2$ とは異なる $z=5$ となる。また、HD21のクラスは、HD20のクラスと同じ $y=1$ として以下説明する。すなわち、HD20、HD21とも、クラス証明書 $Cm1 = KPcm1 // Icm1 // E(Ka, KPcm1 // Icm1)$ およびクラス秘密鍵 $Kcm1$ を保持する。しかしながら、HD21のクラスがHD20のクラスと異なる($y \neq$

1) 場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、HD 20とは異なったものとなる。

図14および図15は、図13に示すライセンスの複製・移動が可能なシステムにおいて、端末装置10のユーザが端末装置10から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置10を介して端末装置10に装着されたHD 20からHD 21へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための第1および第2のフローチャートである。

図14を参照して、端末装置10のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置10のコントローラ108は、バスBS 2およびHDインターフェース部110を介してHD 21へクラス証明書の出力要求を出力する（ステップS 201）。HD 21のコントローラ214は、端子210およびATAインターフェース部212を介してクラス証明書の出力要求を受理すると（ステップS 202）、認証データ保持部202からクラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を読み出し、クラス証明書 C_{m1} をATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS 203）。

端末装置10は、HD 21からクラス証明書 C_{m1} を受理すると（ステップS 204）、受理したクラス証明書 C_{m1} をHD 20へ送信する（ステップS 205）。

HD 20では、端末装置10からHD 21のクラス証明書 C_{m1} を受理すると（ステップS 206）、受理したHD 21のクラス証明書 C_{m1} が正当なクラス証明書であるか否かを検証する（ステップS 207）。検証処理は次のように行なわれる。

HD 20は、HD 21のクラス証明書 $C_{m1} = KP_{cm1} // I_{cm1} // E(K_a, H(KP_{cm1} // I_{cm1}))$ を受理すると、HD 21のクラス証明書 C_{m1} に含まれる署名データ $E(K_a, H(KP_{cm1} // I_{cm1}))$ をHD 20の認証部220において認証鍵 KPa で復号する。そして、認証部220

は、さらに、クラス証明書Cm1に含まれるKPcm1／／Icm1のハッシュ値を演算し、認証部220において復号されたH(KPcm1／／Icm1)の値と比較する。HD20のコントローラ214は、認証部220における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、

5 HD21から受理したクラス証明書Cm1は、正当な証明書であると判断する。

ステップS207において、HD21のクラス証明書Cm1が正当な証明書であると判断されると、HD20のコントローラ214は、HD21のクラス証明書Cm1を承認してHD21のクラス証明書Cm1に含まれるHD21のクラス公開鍵KPcm1を受理し、受理したHD21のクラス公開鍵KPcm1をHD

10 20のセキュアデータ記憶部250内のログメモリ250Bに格納する（ステップS208）。そして、次の処理（ステップS209）へ移行する。コントローラ214は、正当なHD21のクラス証明書でない場合には、HD21のクラス証明書Cm1を非承認として受理せず、エラー通知を端末装置10へ出力する

（図15のステップS252）。そして、端末装置10においてエラー通知が受

15 理されると（図15のステップS253）、配信セッションが終了する。

ステップS207における検証の結果、HD20において、HD21が正当なクラス証明書を持つハードディスクであることが確認され、ステップS208においてHD21のクラス公開鍵KPcm1が受理されると、HD20のセッション鍵発生部226は、セッション鍵Ks1aを生成する（ステップS209）。

20 セッション鍵Ks1aは、認証部220によって得られたHD21のクラス公開鍵KPcm1によって、暗号処理部222において暗号化され、暗号化データE(KPcm1, Ks1a)が生成される（ステップS210）。

そして、コントローラ214は、ライセンスID(LID)および暗号化されたセッション鍵Ks1aを1つのデータ列LID／／E(KPcm1, Ks1

25 a)として、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS211）。

ここで、ライセンスID(LID)は、事前に管理ファイルを参照することでHD20のコントローラ214が取得している。管理ファイルは、HD20に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管

理データを記録したデータファイルであって、ノーマルデータ記憶部270に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

5 端末装置10は、LID//E (K P c m 1, K s 1 a) を受理すると (ステップS212)、受理したLID//E (K P c m 1, K s 1 a) をHD21へ出力する (ステップS213)。そして、HD21のコントローラ214は、端子210およびATAインタフェース部212を介してLID//E (K P c m 1, K s 1 a) を受理する (ステップS214)。続いて、コントローラ214は、バスBS3を介してE (K P c m 1, K s 1 a) を復号処理部230へ与え、
10 復号処理部230は、K c m保持部204に保持されるHD21に固有なクラス秘密鍵K c m 1によって復号処理することにより、セッション鍵K s 1 aを復号し、セッション鍵K s 1 aを受理する (ステップS215)。

HD21のコントローラ214は、HD20で生成されたセッション鍵K s 1 aの受理を確認すると、ATAインターフェース部212および端子210を介してその旨を端末装置10に通知する。端末装置10は、HD21においてセッション鍵K s 1 aが受理された旨の通知を受理すると、HD21において複製・移動動作時に生成されるセッション鍵の生成の要求通知をHD21へ出力する
15 (ステップS216)。HD21のコントローラ214は、端子210およびATAコントローラ212を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部226に対してライセンスの複製・移動時に生成されるセッション鍵の生成を指示する。そして、セッション鍵発生部226は、セッション鍵K s 2 aを生成する (ステップS217)。

セッション鍵発生部226は、セッション鍵K s 2 aを生成すると、バスBS3を介してコントローラ214へ出力し、セッション鍵K s 2 aを受けたコント
25 ローラ214は、ステップS214において受理したライセンスID (LID) とセッション鍵K s 2 aとをHD21のセキュアデータ記憶部250内のログメモリ250Bへ格納し、ステータスST1を「受信待」にする (ステップS218)。

続いて、HD21の暗号処理部224は、切換スイッチ260の接点P bを介

して復号処理部230より与えられるセッション鍵 K_{s1a} によって、切換スイッチ262の接点PdとPfとを順に切換えることによって与えられるセッション鍵 K_{s2a} と個別公開鍵 K_{Pom5} とからなる1つのデータ列を暗号化し、 $E(K_{s1a}, K_{s2a} // K_{Pom5})$ を生成する(ステップS219)。そして、暗号処理部224は、 $E(K_{s1a}, K_{s2a} // K_{Pom5})$ をバスBS3に出力する。バスBS3に出力された暗号化データ $E(K_{s1a}, K_{s2a} // K_{Pom5})$ は、コントローラ214により受理され、コントローラ214は、受理した暗号化データとライセンスID(LID)とを1つのデータ列としたデータ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ をATAインタフェース部212および端子210を介して端末装置10へ出力する(ステップS220)。

そして、端末装置10は、データ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ をHD21から受理すると(ステップS221)、受理したデータをHD20へ出力する(ステップS222)。

HD20は、データ $LID // E(K_{s1a}, K_{s2a} // K_{Pom5})$ を受理すると(ステップS223)、復号処理部228においてセッション鍵 K_{s1a} による復号処理を実行し、HD21で生成されたセッション鍵 K_{s2a} 、およびHD21の個別公開鍵 K_{Pom5} を受理する(ステップS224)。そして、復号処理部228は、復号したセッション鍵 K_{s2a} をバスBS3を介してコントローラ214へ出力し、コントローラ214は、ステップS223において受理したライセンスID(LID)とセッション鍵 K_{s2a} とをHD20のセキュアデータ記憶部250内のログメモリ250Bへ格納し、ステータスST1を「送信待」にする(ステップS225)。

ステップS225の処理を終えると、HD20のコントローラ214は、その旨をATAインタフェース部212および端子210を介して端末装置10に通知する。端末装置10のコントローラ108は、HDインタフェース部110およびバスBS2を介して、HD20からの通知を受理すると、HD20のセキュアデータ記憶部250において、HD20からHD21へ送信するライセンスLICが格納されているLBAをバスBS2およびHDインタフェース11

0を介してHD 20へ出力する（ステップS 2 2 6）。HD 20のコントローラ214は、端子210およびATAインターフェース部212を介して送信対象のライセンスLICの格納先LBAを受理すると（ステップS 2 2 7）、その受理したLBAをセキュアデータ記憶部250のログメモリ250Bに記憶する（ステップS 2 2 8）。

そして、コントローラ214は、受理したLBAに格納されるライセンスLICに対応する有効フラグメモリ250Cのフラグが「有効」であるか「無効」であるかを確認する（ステップS 2 2 9）。コントローラ214は、有効フラグが「有効」であると、受理したLBAに基づいて、そのLBAに格納されるライセンスLICを取得する（ステップS 2 3 0）。

図15を参照して、コントローラ214は、対象のライセンスLICを取得すると、ライセンスLICに含まれるライセンスID（LID）と、ステップS 2 2 3において受理したライセンスID（LID）とを比較し、一致しているか否かをチェックする（ステップS 2 3 1）。コントローラ214は、一致していると判断すると、取得したライセンスLICに含まれる制御情報ACを確認して利用制限がかけられていないかを確認する（ステップS 2 3 2）。

コントローラ214は、制御情報ACにおいてライセンスLICの利用が禁止されていないことを確認すると、取得したライセンスLICを暗号処理部232に与える。暗号処理部232は、復号処理部228によって得られたHD 21の個別公開鍵K P o m 5によってライセンスLICを暗号化して暗号化データE

（K P o m 5， L I C）を生成する（ステップS 2 3 3）。そして、暗号処理部232は、暗号化データE（K P o m 5， L I C）を切替スイッチP cを介して暗号処理部224へ出力し、暗号処理部224は、暗号処理部232から受けた暗号化データを復号処理部228から受けたセッション鍵K s 2 aによって暗号化し、暗号化データE（K s 2 a， E（K P o m 5， L I C））を生成する（ステップS 2 3 4）。

続いて、コントローラ214は、対象のライセンスLICに含まれる制御情報ACに基づいて、HD 20からHD 21へのライセンスLICの送信が「移動」であるか「複製」であるかを確認する（ステップS 2 3 5）。コントローラ21

4は、「移動」であると確認したときは、その対象のライセンスLICに対応する有効フラグメモリ250Cのフラグを「無効」に変更する（ステップS236）。一方、コントローラ214は、「複製」であると確認したときには、当該ライセンスLICがHD20に残っていてもよいので、有効フラグメモリ250Cのフラグの変更は行なわずに次の処理（ステップS237）へ移行する。

コントローラ214は、有効フラグメモリ250Cの処理が終わると、ログメモリ250BのステータスST1を「送信済」に変更し（ステップS237）、ATAインタフェース部212および端子210を介して暗号化データE（Ks2a, E（KPom5, LIC））を端末装置10へ送信する（ステップS238）。

一方、ステップS229において受理したLBAに対応する有効フラグメモリ250Cのフラグが「無効」であったとき、ステップS231においてライセンスID（LID）が一致しないとき、または、ステップS232において、取得したライセンスLICに含まれる制御情報ACにより当該ライセンスLICの利用が禁止されているときは、コントローラ214は、端末装置10に対してエラー通知を出力し（ステップS252）、端末装置10においてエラー通知が受理されると（ステップS253）、処理が終了する。

端末装置10は、ステップS238においてHD20から出力された暗号化データE（Ks2a, E（KPom5, LIC））を受理すると（ステップS239）、受理した暗号化データをHD21へ出力する（ステップS240）。HD21のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データE（Ks2a, E（KPom5, LIC））を受理すると（ステップS241）、バスBS3へ出力する。復号処理部228は、セッション鍵発生部226から与えられたセッション鍵Ks2aを用いてバスBS3に出力されたデータE（Ks2a, E（KPom5, LIC））を復号し、HD21において、ライセンスLICが個別公開鍵KPom5により暗号化された暗号化ライセンスE（KPom5, LIC）が受理される（ステップS242）。そして、復号処理部228は、暗号化ライセンスE（KPom5, LIC）をバスBS3へ出力する。

コントローラ 214 の指示によって、暗号化ライセンス E (K P o m 5, L I C) は、復号処理部 216 において個別秘密鍵 K o m 5 によって復号され、HD 21 においてライセンス L I C が受理される (ステップ S 243)。

5 コントローラ 214 は、ライセンス L I C の受理を確認すると、ATA インターフェース部 212 および端子 210 を介してその旨を端末装置 10 に通知する。端末装置 10 のコントローラ 108 は、HD インターフェース部 110 およびバス B S 2 を介して、HD 21 においてライセンス L I C が受理された旨の通知を受理すると、HD 21 のセキュアデータ記憶部 250 において、その受信したライセンス L I C を格納する L B A をバス B S 2 および HD インターフェース 110
10 を介して HD 21 へ出力する (ステップ S 244)。HD 21 のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介してライセンス L I C の格納先の L B A を受理すると (ステップ S 245)、その受理した L B A をログメモリ 250 B に記憶する (ステップ S 246)。

15 そして、コントローラ 214 は、受理したライセンス L I C に含まれるライセンス I D (L I D) と、ステップ S 214 において受理したライセンス L I D (L I D) とを比較し、一致しているか否かをチェックする (ステップ S 247)。コントローラ 214 は、L I D が一致しており、受理したライセンス L I C が正しいものであると判断すると、端末装置 10 から受理したセキュアデータ記憶部 250 内の L B A に、受理したライセンス L I C を記憶する (ステップ S
20 248)。

25 コントローラ 214 は、指定された L B A にライセンス L I C を記憶すると、有効フラグメモリ 250 C のその L B A に対応するフラグを「有効」にする (ステップ S 249)。そして、コントローラ 214 は、さらに、ログメモリ 250 B のステータス S T 1 を「受信済」にし (ステップ S 250)、複製・移動セッションにおける一連の処理が終了したことを ATA インターフェース部 212 および端子 210 を介して端末装置 10 に通知する。

そして、端末装置 10 において、HD 21 からの処理終了通知が受理されると、HD 20 および HD 21 間の複製・移動セッションが正常終了する。

一方、ステップ S 247 において、コントローラ 214 は、L I D が一致して

おらず、受理したライセンスLICが正しくないと判断すると、ATAインターフェース部212および端子210を介してエラー通知を端末装置10へ出力し（ステップS251）、端末装置10においてエラー通知が受理されると（ステップS253）、複製・移動セッションが終了する。

- 5 ここで、配信セッションのときと同様に、図14および図15に示された複製・移動セッションにおける一連の処理において、ステップS227からステップS252の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

- 10 ここで、図14および図15に示された複製・移動セッションにおいて、ステップS227からステップS235までの処理を再書込処理の対象としたのは、この一連の処理がHD20の内部処理であり、ステップS226の終了後は、ステップS238まで端末装置10においていずれのステップを処理中に処理が中断したかを特定できないため、すべてステップS236が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

- 15 そして、ステップS236からステップS247までの処理を再書込処理の対象としたのは、移動処理の場合、この間は、HD20内のライセンスがステップS236において無効化され、かつ、HD21内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。なお、複製処理の場合は、ステップS236において
20 ライセンスは無効化されないため、移動の場合と同様に再書込処理を行なうようにしても、また、複製処理を最初から行なうようにしてもよい。しかしながら、移動処理の場合は、再書込処理によってのみしかライセンスを復活させることはできない。

- 25 また、ステップS248からステップS250までの処理を再書込処理の対象としたのは、ステップS249、S250については、これらの処理はステップS248におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置10からはステップS248の終了が特定できないため、ステップS248が終了していないものとみなして、ステップS248からステップS250を再書込処理の対象としたものである。なお、ステップS248が終了

していて再書込処理が行なわれた場合には、再書込処理において再書込は拒否される。

また、ステップS 2 5 1の処理を再書込処理の対象としたのは、本来この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置10
5 においては、ステップS 2 5 1において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

なお、端末装置10において、上述したように当該セッションがライセンスの複製であると判断できる場合、あるいはステップS 2 2 7からステップS 2 3 5
10 およびステップS 2 4 9からステップS 2 5 1のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図1 4および図1 5に示された複製・移動セッションを再度実行すればよい。

図1 6から図1 8は、図1 4および図1 5において示した複製・移動セッションの処理フローにおけるステップS 2 2 7からステップS 2 5 2の処理中に異常が発生したときに行なわれる再書込処理の第1から第3のフローチャートである。

図1 6を参照して、端末装置10は、ステップS 2 2 7からステップS 2 5 2
15 の処理中に異常が発生したと判断すると、ライセンスLICの再送要求をHD 2 0へ出力する（ステップS 3 0 1）。HD 2 0のコントローラ2 1 4は、端子2 1 0およびATAインターフェース部2 1 2を介して再送要求を受理すると、セキュアデータ記憶部2 5 0内のログメモリ2 5 0 Bに格納されているステータス
20 ST 1の状態を確認する（ステップS 3 0 2）。コントローラ2 1 4は、ステータスST 1が「送信待」または「送信済」でないとき、すなわち複製・移動セッションにおいてライセンスLICの送信側でないときは、図1 8に示すステップS 3 7 1へ処理が移行する。

HD 2 0のコントローラ2 1 4は、ステータスST 1が「送信待」または「送信済」であるときは、セッション鍵発生部2 2 6にセッション鍵を生成するよう
25 に指示し、セッション鍵発生部2 2 6は、セッション鍵K s 1 bを生成する（ステップS 3 0 3）。セッション鍵K s 1 bが生成されると、コントローラ2 1 4は、中断以前に受理してログメモリ2 5 0 Bに格納されたHD 2 1のクラス公開鍵K P c m 1を取得する（ステップS 3 0 4）。そして、そのHD 2 1のクラス

公開鍵 K_{Pcm1} によって、セッション鍵 K_{s1b} が暗号処理部 222 によって暗号化され、暗号化データ $E(K_{Pcm1}, K_{s1b})$ が生成される (ステップ S305)。コントローラ 214 は、生成された暗号化データ $E(K_{Pcm1}, K_{s1b})$ を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S306)。

端末装置 10 は、暗号化データ $E(K_{Pcm1}, K_{s1b})$ を受領すると (ステップ S307)、受領した暗号化データ $E(K_{Pcm1}, K_{s1b})$ を HD 21 へ出力する (ステップ S308)。HD 21 のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介して $E(K_{Pcm1}, K_{s1b})$ を受領すると (ステップ S309)、バス BS3 を介して $E(K_{Pcm1}, K_{s1b})$ を復号処理部 230 へ与える。そうすると、復号処理部 230 は、 K_{cm} 保持部 204 に保持される HD 21 に固有なクラス秘密鍵 K_{cm1} によって復号処理を実行してセッション鍵 K_{s1b} を復号し、セッション鍵 K_{s1b} を受領する (ステップ S310)。

HD 21 のコントローラ 214 は、HD 20 で生成されたセッション鍵 K_{s1b} の受領を確認すると、ATA インターフェース部 212 および端子 210 を介してその旨を端末装置 10 に通知する。端末装置 10 のコントローラ 108 は、HD インターフェース部 110 およびバス BS2 を介して HD 21 からの通知を受領すると、HD 21 のログメモリ 250B に格納されるログの HD 20 への出力要求をバス BS2 および HD インターフェース部 110 を介して HD 21 へ出力する (ステップ S311)。HD 21 のコントローラ 214 は、端子 210 および ATA コントローラ 212 を介してログの出力要求通知を受領すると (ステップ S312)、ログメモリ 250B に格納された LBA に記憶されるライセンス LIC のライセンス ID (LID) と、ログメモリ 250B に格納されたライセンス ID (LID) とが一致するか否かを確認する (ステップ S313)。

コントローラ 214 は、ライセンス ID (LID) が一致すると、さらに、ログメモリ 250B に格納された LBA に記憶されるライセンス LIC に対応する有効フラグメモリ 250C のフラグを確認し、そのライセンス LIC が有効であるか無効であるかを確認する (ステップ S314)。コントローラ 214 は、有

効フラグメモリ 250C のフラグが「有効」であるときは、ログメモリ 250B のステータス ST2 を「データ有」に変更し（ステップ S315）、次の処理（ステップ S318）へ移行する。一方、コントローラ 214 は、有効フラグメモリ 250C のフラグが「無効」であるときは、ログメモリ 250B のステータス ST2 を「移動済」に変更し（ステップ S316）、次の処理（ステップ S318）へ移行する。

また、コントローラ 214 は、ステップ S313 において両ライセンス ID（LID）が一致しないときは、ログメモリ 250B のステータス ST2 を「データ無」に変更する（ステップ S317）。

このように、複製・移動セッションにおいても、ログメモリ 250B に格納された LBA を用いて、その LBA により指定されるライセンスメモリ 250A の記憶位置に記憶されるライセンスのライセンス ID（LID）を LBA に基づいて直接確認できるので、ライセンスメモリ 250A に相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしにライセンス ID（LID）の特定または有無を判断することができる。

ステータス ST2 の変更処理がなされると、コントローラ 214 は、ログメモリ 250B からライセンス ID（LID）、ステータス ST1、ST2 およびセッション鍵 Ks2c を取得する（ステップ S318）。ここで、ログメモリ 250B に格納されているセッション鍵は Ks2a であるが、表記の関係上、ログメモリ 250B から取得したセッション鍵を Ks2c としている。そして、コントローラ 214 は、取得したセッション鍵 Ks2c をバス BS3 を介して暗号処理部 224 へ出力する。

暗号処理部 224 は、切換スイッチ 260 の接点 Pb を介して復号処理部 230 より与えられるセッション鍵 Ks1b によってセッション鍵 Ks2c を暗号化し、E（Ks1b, Ks2c）生成する（ステップ S319）。そして、暗号処理部 224 は、生成した E（Ks1b, Ks2c）をバス BS3 に出力する。バス BS3 に出力された E（Ks1b, Ks2c）は、コントローラ 214 により受理され、コントローラ 214 は、ステップ S318 において取得したデータとともに 1 つの受信ログ LID // E（Ks1b, Ks2c） // ST1 // ST

2を生成し、そのハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ を生成する(ステップS320)。そして、コントローラ214は、ハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ をバスBS3を介して暗号処理部224へ出力する。

- 5 暗号処理部224は、切換スイッチ260の接点Pbを介して復号処理部230より与えられるセッション鍵 $Ks1b$ によって、バスBS3から取得したハッシュ値 $H(LID // E(Ks1b, Ks2c) // ST1 // ST2)$ を暗号化し、署名データ $E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を生成する(ステップS321)。そして、暗号処理部224は、生成した $E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ をバスBS3に出力する。

- 10 コントローラ214は、バスBS3から署名データを取得すると、ステップS318において取得した受信ログを用いて、署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を生成し、ATAインターフェース部212および端子210を介して端末装置10へ出力する(ステップS322)。

- 15 端末装置10は、署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ をHD21から受理すると(ステップS323)、受理したデータをHD20へ出力する(ステップS324)。

- 20 HD20は、署名付き受信ログ $LID // E(Ks1b, Ks2c) // ST1 // ST2 // E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を受理すると(ステップS325)、受理したデータの検証を行なう(ステップS326)。検証処理は、以下のように行われる。

25 HD20のコントローラ214は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データ $E(Ks1b, H(LID // E(Ks1b, Ks2c) // ST1 // ST2))$ を復号処理部228へ出力する。そして、復号処理部228は、ステップS303で生成したセッション

- 鍵 K_{s1b} によって署名データ $E(K_{s1b}, H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2))$ を復号する。一方、HD20のコントローラ214は、署名付き受信ログの前半部である受信ログ $LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2$ のハッシュ値を演算し、復号処理部228により復号された $H(LID // E(K_{s1b}, K_{s2c}) // ST1 // ST2)$ の値と比較する。HD20のコントローラ214は、復号処理部228における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、HD21から受理したデータ列は、正当なデータを含むものとしてHD20において認証される。
- 10 ステップS326において署名付き受信ログの検証が行なわれ、そのデータがHD20において承認されると、HD20のコントローラ214は、ステップS325において受理したデータに含まれるライセンスID(LID)をログメモリ250Bに格納されるライセンスID(LID)と比較する(ステップS327)。
- 15 コントローラ214は、ライセンスID(LID)が一致すると、受信したデータ列に含まれる暗号データ $E(K_{s1b}, K_{s2c})$ を復号処理部228へ出力し、復号処理部228は、セッション鍵 K_{s1b} によって復号し、セッション鍵 K_{s2c} を受理する(ステップS328)。そして、復号されたセッション鍵 K_{s2c} は、バスBS3を介してコントローラ214へ出力される。続いて、コントローラ214は、エラー発生時のセッション鍵 K_{s2a} を今回受理したセッション鍵 K_{s2c} と比較チェックする(ステップS329)。コントローラ214は、セッション鍵 K_{s2a} とセッション鍵 K_{s2c} とが一致していると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS330)。
- 20 HD20のコントローラ214は、エラー発生時のセッション鍵 K_{s2a} を今回受理したセッション鍵 K_{s2c} と比較チェックする(ステップS329)。コントローラ214は、セッション鍵 K_{s2a} とセッション鍵 K_{s2c} とが一致していると判断すると、受理したステータスST1, ST2の内容を確認する(ステップS330)。
- 25 HD20のコントローラ214は、受信したステータスST1が「受信待」であり、ステータスST2が「データ無」であるとき、HD21に送信したはずのライセンスLICが何らかの異常によりHD21において受理されていないと判断する。そうすると、HD20のコントローラ214は、さらに、ログメモリ250Bに格納されたLBAに記憶されるライセンスLICのライセンスID(L

５ ID) と、ログメモリ 250B に格納されたライセンス ID (LID) とが一致するか否かを確認する (ステップ S331)。HD20 のコントローラ 214 は、ライセンス ID (LID) が一致すると、さらに、ログメモリ 250B に格納された LBA に対応する有効フラグメモリ 250C のフラグを確認し、そのライセンス LIC が有効であるか無効であるかを確認する (ステップ S332)。そして、コントローラ 214 は、有効フラグメモリ 250C のフラグが「無効」であるときは、その有効フラグメモリ 250C のフラグを「有効」に変更する (ステップ S333)。一方、コントローラ 214 は、有効フラグメモリ 250C のフラグが「有効」であるときは、次の処理 (ステップ S334) へ移行する。そして、コントローラ 214 は、ログメモリ 250B に格納される LBA を取得し、ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する (ステップ S334)。

１５ 端末装置 10 のコントローラ 108 は、HD20 から HD インターフェース部 110 およびバス BS2 を介して対象のライセンス LIC が格納される LBA を受理すると (ステップ S335)、HD21 において複製・移動動作時に生成されるセッション鍵の生成の要求通知をバス BS2 および HD インターフェース部 110 を介して HD21 へ出力する (ステップ S336)。

２０ HD21 は、端末装置 10 からセッション鍵の生成要求通知を受理すると、以下、図 14 および図 15 において説明したステップ S217 から処理終了までの一連の処理において、セッション鍵 Ks2a に代えて新たなセッション鍵 Ks2b が生成され、そのセッション鍵 Ks2b が使用されるほかは、同様の処理が行なわれる。したがって、ステップ S336 に続く一連の処理の説明は繰返しになるので省略する。

２５ なお、ステップ S335 において処理を終了し、HD20 にライセンスを残すことも可能である。この場合、図 14 および図 15 に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

なお、図 16 ～図 18 のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップ S301 ～ S344 およびステップ S347 ～ S371 のいずれかのステップにおいて処理が中断した場合に

は、再び図 1 6 ～図 1 8 に示されるフローチャートにしたがって再書込処理を行なうことができる。一方、ステップ S 3 2 5 ～S 3 4 6 のいずれかのステップにおいて処理が中断した場合には、図 1 4 および図 1 5 のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

このようにして、端末装置 1 0 に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先の HD 2 1 から受取ったクラス証明書 C m 1 が有効であることを確認し、クラス証明書 C m 1 に含まれて送信されたクラス公開鍵 K P c m 1 によってライセンスの複製・移動が行なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンスの複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置である HD 2 1 における複製・移動セッションの対象となったライセンス L I C に対する受信ログを送信側のデータ記憶装置である HD 2 0 へ送信し、HD 2 0 において、自身のログメモリ 2 5 0 B に記憶される内容と、ログメモリ 2 5 0 B に記憶される L B A によって特定されるライセンスメモリ 2 5 0 A に記憶されるライセンス L I C とを比較し、さらに有効フラグメモリ 2 5 0 C に記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、2 つのデータ記憶装置 HD 2 0 および HD 2 1 に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

その上、受信側のデータ記憶装置である HD 2 1 においてライセンスを記憶する L B A の指示がなされた場合において、その L B A をログの一部として記録することによって、複製・移動セッション中に異常が発生したとき、ログメモリ 2 5 0 B に格納された L B A にしたがって、そのセッションによって記録されるべ

きライセンスLICのライセンスメモリ250Aにおける記憶状態を、相当数のライセンスを記録できるライセンスメモリ250A内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、複製・移動処理においても迅速な再書込処理を行なうことができる。また、送信側

5 側のデータ記憶装置であるHD20においても、ダイレクトに処置の対象であるライセンスLICの内容および状態（利用可否）が判断できる。

このように、本発明は、複製・移動セッションの中断によるライセンスLICの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、

10 確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

なお、図14～図18におけるHD21の処理ステップS202, 203, S214, S215, S217～S220, S241～S243, S245～S251, S309, S310, S312～S322, S337～S340, S361～S363, S365～S371は、図8～図12におけるHD20の処理ステップS2, S3, S16, S17, S19～S22, S33～S35, S37～S43, S109, S110, S112～S122, S136～S139, S150～S152, S154～S160とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるHD21の処理とライセンスの配信処理時におけるHD20の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（HD20, HD21）においてライセンスを書込むためのデータ記憶装置における処理である。

15

20

なお、署名付き受信ログについては、配信処理と同様に、LID//ST1//ST2//H(Ks1b//LID//Ks2c//ST1//ST2)とすることも可能である。

25

〔再生許諾〕

再び図5を参照して、コンテンツデータを再生する再生回路150を備えた端末装置10にデータ記憶装置としてのHD20が装着され、コンテンツデータの再生許諾は、HD20から端末装置10内の再生回路150に対して行なわれる。

図19は、端末装置10のユーザが端末装置10から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置10に装着されたHD20から端末装置10内の再生回路150へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

- 5 図19を参照して、端末装置10のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置10のコントローラ108は、バスBS2を介して再生回路150へクラス証明書の出力要求を出力する（ステップS401）。再生回路150において、認証データ保持部1502は、バスBS2からクラス証明書の出力要求を受けると（ステップS402）、保持しているクラス証明書 $Cp3 = KPcp3 // Ic p3 // E(Ka, H(KPcp3 // Ic p3))$ をバスBS2へ出力する（ステップS403）。

コントローラ108は、バスBS2からクラス証明書 $Cp3$ を受理すると（ステップS404）、受理したクラス証明書 $Cp3$ をバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS405）。

- 15 HD20では、端末装置10からクラス証明書 $Cp3$ を受理すると（ステップS406）、受理したクラス証明書 $Cp3$ が正当なクラス証明書であるか否かを検証する（ステップS407）。検証処理は、複製・移動セッションにおけるステップS207において説明したのと同様の方法で行なわれ、説明は省略する。

- 20 ステップS407において、クラス証明書 $Cp3$ が正当な証明書であると判断された場合、コントローラ214は、クラス証明書 $Cp3$ を承認し、クラス証明書 $Cp3$ に含まれるクラス公開鍵 $KPcp3$ を受理する（ステップS408）。そして、次の処理（ステップS409）へ移行する。コントローラ214は、正当なクラス証明書でない場合には、クラス証明書 $Cp3$ を非承認とし、クラス証明書 $Cp3$ を受理せずにエラー通知を端末装置10へ出力し（ステップS435）、
25 5）、端末装置10においてエラー通知が受理されると（ステップS436）、再生許諾セッションが終了する。

ステップS407における検証の結果、HD20において、再生回路150が正当なクラス証明書を持つ再生回路であることが確認され、ステップS408においてクラス公開鍵 $KPcp3$ が受理されると、HD20のセッション鍵発生部

226は、セッション鍵 K_{s1d} を生成する（ステップS409）。セッション鍵 K_{s1d} は、受理されたクラス公開鍵 K_{Pcp3} によって、暗号処理部222において暗号化され、暗号化データ $E(K_{Pcp3}, K_{s1d})$ が生成される（ステップS410）。

5 そして、コントローラ214は、暗号処理部222からバスBS3を介して暗号化データ $E(K_{Pcp3}, K_{s1d})$ を受けると、ATAインターフェース部212および端子210を介して端末装置10へ出力する（ステップS411）。

10 端末装置10において、HDインターフェース部110およびバスBS2を介してコントローラ108が暗号データ $E(K_{Pcp3}, K_{s1d})$ を受理すると（ステップS412）、コントローラ108は、受理した暗号化データ $E(K_{Pcp3}, K_{s1d})$ をバスBS2を介して再生回路150へ出力する（ステップS413）。再生回路150の復号処理部1506は、バスBS2から暗号化データ $E(K_{Pcp3}, K_{s1d})$ を受理すると（ステップS414）、 K_{cp} 保持部1504に保持される再生回路150に固有なクラス秘密鍵 K_{cp3} によって復号処理することによりセッション鍵 K_{s1d} を復号し、セッション鍵 K_{s1d} が受理される（ステップS415）。

15 セッション鍵 K_{s1d} が受理されると、セッション鍵発生部1508は、セッション鍵 K_{s2d} を生成し（ステップS416）、生成したセッション鍵 K_{s2d} を暗号処理部1510に与える。暗号処理部1510は、復号処理部1506から受けるセッション鍵 K_{s1d} をセッション鍵 K_{s2d} により暗号化し、暗号化データ $E(K_{s1d}, K_{s2d})$ を生成する（ステップS417）。そして、暗号処理部1510は、暗号化データ $E(K_{s1d}, K_{s2d})$ をバスBS2へ出力する（ステップS418）。

20 コントローラ108は、バスBS2から暗号化データ $E(K_{s1d}, K_{s2d})$ を受理し（ステップS419）、受理したデータをバスBS2およびHDインターフェース部110を介してHD20へ出力する（ステップS420）。

25 HD20のコントローラ214は、端子210およびATAインターフェース部212を介して暗号化データ $E(K_{s1d}, K_{s2d})$ を受理すると（ステップS421）、受理したデータをバスBS3へ出力する。復号処理部228は、

セッション鍵発生部 226 から与えられたセッション鍵 K_{s1d} を用いてバス $BS3$ に出力された暗号化データ $E(K_{s1d}, K_{s2d})$ を復号し、 $HD20$ においてセッション鍵 K_{s2d} が受理される (ステップ $S422$)。そして、コントローラ 214 は、セッション鍵 K_{s2d} が受理されると、その旨の通知を ATA インターフェース部 212 および端子 210 を介して端末装置 10 へ出力する。

端末装置 10 のコントローラ 108 は、 HD インターフェース部 110 およびバス $BS2$ を介して $HD20$ においてセッション鍵 K_{s2d} が受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンス LIC が格納されているライセンスメモリ 250A の LBA をバス $BS2$ および HD インターフェース部 110 を介して $HD20$ へ出力する。

$HD20$ のコントローラ 214 は、端子 210 および ATA インターフェース部 212 を介して対象のライセンス LIC が格納されている LBA を受理すると (ステップ $S424$)、その LBA に格納されるライセンス LIC に対応する有効フラグメモリ 250C のフラグが「有効」であるか「無効」であるかを確認する (ステップ $S425$)。

コントローラ 214 は、有効フラグメモリ 250C のフラグが「有効」であると、受理した LBA に基づいて、対象のライセンス LIC をライセンスメモリ 250A から取得する (ステップ $S426$)。そして、コントローラ 214 は、取得したライセンス LIC に含まれる制御情報 AC の内容を確認する (ステップ $S427$)。コントローラ 214 は、制御情報 AC において利用回数が指定されているときは、制御情報 AC の利用回数を 1 増分し、次の処理 (ステップ $S429$) へ移行する。一方、コントローラ 214 は、制御情報 AC により再生制限がかけられていないときは、取得したライセンス LIC に含まれるコンテンツ鍵 K_c をバス $BS3$ へ出力する。

暗号処理部 224 は、復号処理部 228 から受けるセッション鍵 K_{s2d} によりバス $BS3$ 上に出力されたコンテンツ鍵 K_c を暗号化して暗号化データ $E(K_{s2d}, K_c)$ を生成し (ステップ $S429$)、生成したデータをバス $BS3$ へ出力する。そして、コントローラ 214 は、バス $BS3$ 上に出力された暗号化データ $E(K_{s2d}, K_c)$ を ATA インターフェース部 212 および端子 210

を介して端末装置 10 へ出力する（ステップ S 4 3 0）。

端末装置 10 のコントローラ 108 は、HD インターフェース部 110 およびバス B S 2 を介して暗号化データ E（K s 2 d，K c）を受理すると（ステップ S 4 3 1）、受理したデータをバス B S 2 へ出力する（ステップ S 4 3 2）。

5 再生回路 150 の復号処理部 1512 は、バス B S 2 から暗号化データ E（K s 2 d，K c）を受理すると（ステップ S 4 3 3）、セッション鍵発生部 1508 から与えられるセッション鍵 K s 2 d を用いて暗号化データ E（K s 2 d，K c）を復号する。これにより、再生回路 150 においてコンテンツ鍵 K c が受理され（ステップ S 4 3 4）、一連の再生許諾セッションの処理が正常終了する。

10 一方、ステップ S 4 2 5 において、有効フラグメモリ 250C のフラグが「無効」であったとき、またはステップ S 4 2 7 において、制御情報 A C に含まれる内容が再生不可であったときは、コントローラ 214 は、端末装置 10 に対してエラー通知を出力し（ステップ S 4 3 5）、端末装置 10 においてエラー通知が受理されると（ステップ S 4 3 6）、再生許諾セッションが終了する。

15 このようにして、データ記憶装置である HD 20 から端末装置 10 に備えられる再生回路 150 への再生許諾に関しても、再生回路 150 が正規のクラス証明書 C p 3 を保持していること、およびクラス証明書 C p 3 に含まれて送信されたクラス公開鍵 K P c p 3 が有効であることを確認した上でコンテンツ鍵 K c が再生回路 150 へ送信され、不正なコンテンツデータの再生を禁止することができる。

20 また、上述したように、ハードディスクにおいて相当数記憶されるライセンスを L B A により管理することによって、再生許諾セッションにおいて、再生リクエストのあったコンテンツデータに対応するライセンスを、相当数のデータの中から検索することなくダイレクトに取得することができ、迅速な処理が実現できる。

25 なお、フローチャートにおいて図示しないが、再生回路 150 は、コンテンツの再生許諾がなされ、コンテンツ鍵 K c を受理すると、HD 20 から出力された暗号化コンテンツデータ E（K c，D c）を復号処理部 1514 において復号し、再生部 1516 において復号処理部により復号されたデータ D c が再生され、D

A変換部1518によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子1520へ再生信号が出力される。

5 なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

10 今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

産業上の利用可能性

15 以上のように、この発明によるデータ記憶装置は、デジタルデータ化された機密データの著作権保護を必要とするデータ配信システムにおけるデータ記憶装置として有用であり、特に、機密データを暗号化した暗号化機密データの再生に際して必要とされるライセンス（復号鍵および利用規則）を安全に入出力し、かつ、多数のライセンスを記憶することが必要なデータ記憶装置に適し、さらには、保護を必要とする機密データを安全に入出力し、かつ、機密データの入出力の中断
20 から安全に入出力を再開することが必要なデータ記憶装置に適している。

請求の範囲

1. 機密データ（L I C）を保護するための所定の入出力手順に従って前記機密データ（L I C）の入出力を行ない、かつ、前記機密データ（L I C）を記憶するデータ記憶装置であって、
- 5 外部とデータのやり取りを行なうインターフェース部（212）と、
前記機密データ（L I C）を記憶する第1の記憶部（250A）と、
前記所定の入出力手順に従った前記機密データ（L I C）の入出力に関するログ情報と入出力の対象となる前記機密データ（L I C）の前記第1の記憶部（250A）における記憶位置を示すアドレスとを記憶する第2の記憶部（250B）とを備えるデータ記憶装置。
- 10 2. 前記機密データ（L I C）の入出力を制御する制御部（214）をさらに備え、
前記ログ情報は、
- 15 入出力の対象となる前記機密データ（L I C）を識別する識別コード（L I D）と、
入出力の対象となる前記機密データ（L I C）の前記第1の記憶部（250A）における記憶状態を示す第1のステータス（S T 2）とを含み、
前記制御部（214）は、前記所定の入出力手順に従って、入出力の対象となる前記機密データ（L I C）の前記識別コード（L I D）と前記アドレスとを前記インターフェース部（212）を介して受取ると前記第2の記憶部（250B）に記憶し、前記インターフェース部（212）を介して受ける外部からの要求に応じて、前記第2の記憶部（250B）に記憶された前記識別コード（L I D）と前記アドレスとに基づいて前記第1の記憶部（250A）における前記機密データ（L I C）の記憶状態を確認し、前記記憶状態に基づいて前記第1のステータス（S T 2）を更新する、請求項1に記載のデータ記憶装置。
- 20 3. 前記ログ情報は、入出力の対象となった前記機密データ（L I C）の入出力における前記所定の入出力手順の進行状態を記録する第2のステータス（S T 1）をさらに含み、
- 25

前記制御部（２１４）は、前記所定の入出力手順の進行に応じて前記第２のステータス（ＳＴ１）を更新する、請求項２に記載のデータ記憶装置。

４． 前記ログ情報は、前記所定の入出力手順を特定する手順特定情報（Ｋｓ２ｘ）をさらに含み、

５ 前記制御部（２１４）は、前記手順特定情報（Ｋｓ２ｘ）を新たに取得するごとに前記手順特定情報（Ｋｓ２ｘ）を更新する、請求項２に記載のデータ記憶装置。

５． 前記所定の入出力手順に従って、前記インターフェース部（２１２）を介して前記機密データ（ＬＩＣ）の提供元または提供先との間に暗号通信路を確立し、前記確立された暗号通信路を用いて前記機密データ（ＬＩＣ）の受信または送信を行なう暗号通信部（２６８）をさらに備え、

前記所定の入出力手順の１つであって、前記機密データ（ＬＩＣ）を受信して記憶する入力手順において、

前記暗号通信部（２６８）は、前記入力手順に従って前記機密データ（ＬＩＣ）を受信し、

前記制御部（２１４）は、前記インターフェース部（２１２）を介して前記アドレスを受取ると前記第２の記憶部（２５０Ｂ）に前記受取ったアドレスを記憶し、前記受取ったアドレスによって特定される前記第１の記憶部（２５０Ａ）上の記憶位置に前記暗号通信部（２６８）が受信した前記機密データ（ＬＩＣ）を記憶する、請求項４に記載のデータ記憶装置。

６． 前記入力手順において、

前記暗号通信部（２６８）は、第１のセッション鍵（Ｋｓ２ａ）を生成し、

前記制御部（２１４）は、前記暗号通信部（２６８）によって前記第１のセッション鍵（Ｋｓ２ａ）が生成されるごとに、前記第１のセッション鍵（Ｋｓ２ａ）によって前記手順特定情報（Ｋｓ２ｘ）を更新する、請求項５に記載のデータ記憶装置。

７． 前記ログ情報または前記ログ情報の一部に対して電子署名を施した署名付きログ情報（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ

2))) を生成する署名部 (2 2 4 , 2 1 4) をさらに備え、

前記所定の入出力手順の1つであって、前記入力手順が中断した場合にその中断した入力手順を復元する再入力手順において、

5 前記制御部 (2 1 4) は、前記第2の記憶部 (2 5 0 B) に記憶された前記ログ情報に含まれる前記第1のステータス (S T 2) を更新し、前記ログ情報を前記第2の記憶部 (2 5 0 B) から取得して前記署名部 (2 2 4 , 2 1 4) に与え、

前記署名部 (2 2 4 , 2 1 4) は、前記更新された第1のステータス (S T 2) が含まれる前記ログ情報を受取って前記署名付きログ情報を生成し、

10 前記暗号通信部 (2 6 8) は、前記再入力手順に従って、前記署名部 (2 2 4 , 2 1 4) によって生成された前記署名付きログ情報を前記確立された暗号通信路を用いて送信する、請求項5に記載のデータ記憶装置。

8. 前記所定の入出力手順の1つであって、前記第1の記憶部 (2 5 0 A) に記憶された前記機密データ (L I C) を外部へ出力する出力手順において、

15 前記制御部 (2 1 4) は、前記インターフェース部 (2 1 2) を介して前記アドレスを受取ると前記第2の記憶部 (2 5 0 B) に前記受取ったアドレスを記憶し、前記受取ったアドレスによって特定される前記第1の記憶部 (2 5 0 A) 上の記憶位置から前記機密データ (L I C) を取得して前記暗号通信部 (2 6 8) へ与え、

20 前記暗号通信部 (2 6 8) は、前記出力手順に従って、前記制御部 (2 1 4) から与えられた前記機密データ (L I C) を送信する、請求項5に記載のデータ記憶装置。

9. 前記出力手順において、

前記暗号通信部 (2 6 8) は、外部で生成された第2のセッション鍵 (K s 2 a) を受信し、

25 前記制御部 (2 1 4) は、前記暗号通信部 (2 6 8) が前記第2のセッション鍵 (K s 2 a) を受信するごとに、前記受信した第2のセッション鍵 (K s 2 a) によって前記手順特定情報 (K s 2 x) を更新する、請求項8に記載のデータ記憶装置。

10. 外部から受信した署名付きログ情報 (L I D / / E (K s 1 b , K s 2

c) $\text{ST1} \text{ ST2} \text{ E} (\text{Ks1b}, \text{H} (\text{LID} \text{ E} (\text{Ks1b}, \text{Ks2c}) \text{ ST1} \text{ ST2}))$ の正当性を検証して認証するログ認証部 (228, 214) をさらに備え、

5 前記所定の入出力手順の1つであって、前記出力手順が中断した場合にその中断した出力手順を復元する再出力手順において、

前記暗号通信部 (268) は、前記再出力手順に従って、前記署名付きログ情報を受信して前記ログ認証部 (228, 214) に与え、

前記ログ認証部 (228, 214) は、前記暗号通信部 (268) から受信した前記署名付きログ情報を検証し、

10 前記制御部 (214) は、前記受信した署名付きログ情報が正当であると認証されたとき、前記第2の記憶部 (250B) に記憶された前記ログ情報と前記受信した署名付きログ情報とに基づいて前記出力手順が中断したか否かを判断し、前記出力手順が中断したと判断したとき、前記第2の記憶部 (250B) に記憶された前記アドレスによって特定される前記第1の記憶部 (250A) 上の記憶位置を前記出力手順が中断する前の記憶状態に復元可能か否かを判断し、復元可能と判断したとき、前記出力手順が中断する前の記憶状態に前記記憶位置を復元し、前記中断された出力手順を再開する、請求項8に記載のデータ記憶装置。

11. 前記機密データ (LIC) は、その機密データ (LIC) に固有の前記識別コード (LID) を含み、

20 前記制御部 (214) は、前記第1の記憶部 (250A) における前記機密データ (LIC) の記憶状態を確認するとき、前記アドレスによって特定される前記第1の記憶部 (250A) 上の記憶位置に記憶されている前記機密データ (LIC) に含まれる前記識別コード (LID) によって前記機密データ (LIC) を特定する、請求項2に記載のデータ記憶装置。

25 12. 前記所定の入出力手順の1つであって、前記機密データ (LIC) を前記インターフェース部 (212) を介して受取って前記第1の記憶部 (250A) に記憶する入力手順において、

前記制御部 (214) は、前記受取った機密データ (LIC) に含まれる識別コード (LID) と前記ログ情報に含まれる識別コード (LID) とが一致しな

いとき、前記機密データ（L I C）を前記第 1 の記憶部（2 5 0 A）に記憶することなく、前記入力手順を中止する、請求項 1 1 に記載のデータ記憶装置。

1 3. 前記所定の入出力手順の 1 つであって、前記第 1 の記憶部（2 5 0 A）に記憶された前記機密データ（L I C）を前記インターフェース部（2 1 2）を介して出力する出力手順において、

前記制御部（2 1 4）は、前記アドレスによって特定される前記第 1 の記憶部（2 5 0 A）上の記憶位置に記憶されている前記機密データ（L I C）に含まれる識別コード（L I D）と前記ログ情報に含まれる識別コード（L I D）とが一致しないとき、前記機密データ（L I C）の出力を行なうことなく、前記出力手順を中止する、請求項 1 1 に記載のデータ記憶装置。

1 4. 前記ログ情報に対する署名データ（E（K s 1 b, H（L I D／／E（K s 1 b, K s 2 c）／／S T 1／／S T 2）））を生成し、前記生成した署名データを前記ログ情報に添付した署名付きログ情報を生成する署名部（2 2 4, 2 1 4）をさらに備え、

前記機密データ（L I C）を前記インターフェース部（2 1 2）を介して受取って前記第 1 の記憶部（2 5 0 A）に記憶する入力手順が中断した場合、中断した前記入力手順を再開する再入力手順において、

前記制御部（2 1 4）は、前記署名部（2 2 4, 2 1 4）によって生成された前記署名付きログ情報を前記インターフェース部（2 1 2）を介して出力する、請求項 2 に記載のデータ記憶装置。

1 5. 前記インターフェース部（2 1 2）を介して前記機密データ（L I C）の提供先から受取った、前記提供先のもう 1 つのログ情報に対する署名データ（E（K s 1 b, H（L I D／／E（K s 1 b, K s 2 c）／／S T 1／／S T 2）））が前記もう 1 つのログ情報に添付されたもう 1 つの署名付きログ情報の正当性を検証して認証するログ認証部（2 2 8, 2 1 4）をさらに備え、

前記第 1 の記憶部（2 5 0 A）に記憶された前記機密データ（L I C）を前記インターフェース部（2 1 2）を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証部（2 2 8, 2 1 4）は、前記中断した出力手順における前記機

密データ（L I C）の提供先から受取った前記もう 1 つの署名付きログ情報の正当性を検証し、

5 前記制御部（2 1 4）は、前記もう 1 つの署名付きログ情報が正当でないと認証されたとき、または、前記もう 1 つの署名付きログ情報が正当であると認証され、かつ、前記もう 1 つの署名付きログ情報と前記第 2 の記憶部（2 5 0 B）に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項 1 4 に記載のデータ記憶装置。

1 6 . 前記機密データ（L I C）は、暗号化されたコンテンツデータ（E（K c , D c））を復号して利用するための復号鍵であって、

10 前記暗号化されたコンテンツデータ（E（K c , D c））を記憶するための第 3 の記憶部（2 7 0）をさらに備える、請求項 1 に記載のデータ記憶装置。

FIG. 1

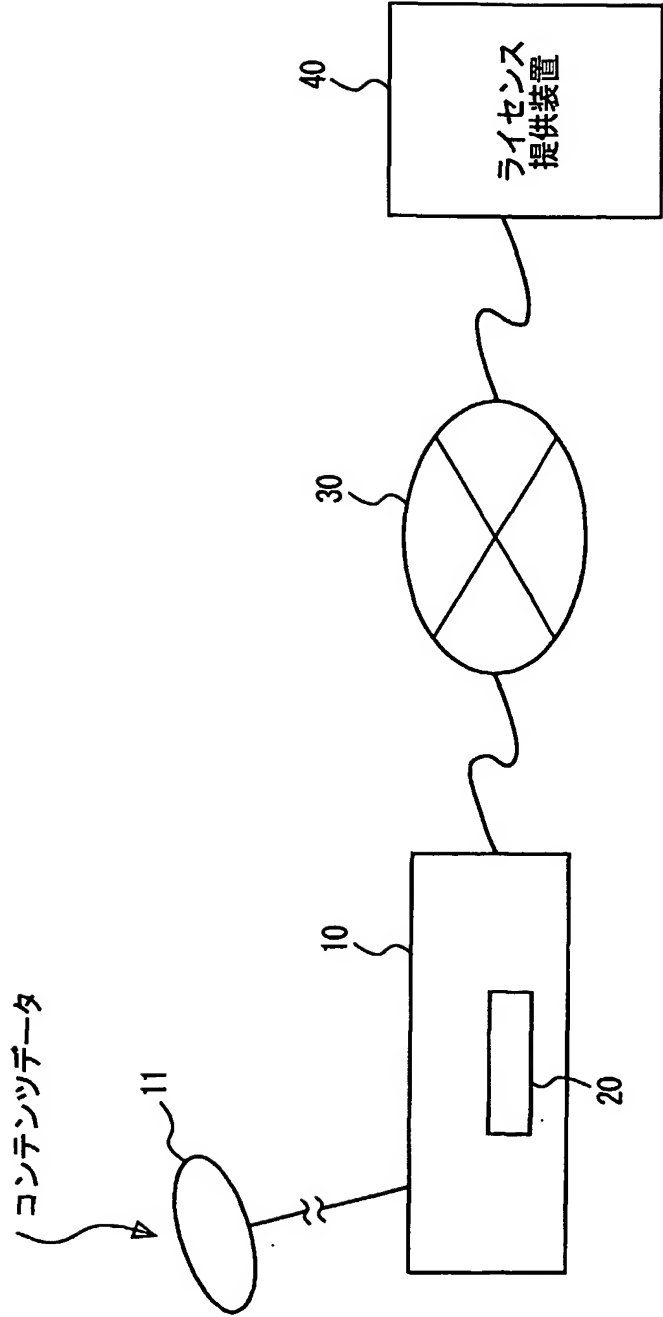


FIG. 2

記号	名称	属性	特性
Dc	データ	データ固有	例：映像データ、音楽データ、朗読データ、教材データ、 画像データ、ゲームプログラム Kclにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dclに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

FIG. 3

記号	名称	特性
ライセンス提供装置	KPa 認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンスト提供側にて運用される
	Ks1x セッション鍵	ライセンストの配信ごとに生成される一時鍵 共通鍵
	KPa 認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンスト提供側にて運用される
	KPcmy クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 [y]はクラスを識別するための識別子
	Kcmy クラス秘密鍵	クラス公開鍵KPcmyにて暗号化されたデータを復号する非対称な復号鍵
データ記録装置 (ハードディスク)	lcmv クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Qmy クラス証明書	$Qmy = KPcmy // lcmv // E(Ka, H(KPcmy // lcmv))$ 認証鍵KPaによってその正当性が確認できる
	KPomz 個別公開鍵	データ記録装置ごとに管理される暗号鍵 [z]はデータ記録装置を識別するための識別子
	Komz 個別秘密鍵	個別公開鍵KPomzにて暗号化されたデータを復号する非対称な復号鍵
	Ks1x セッション鍵	ライセンストの授受ごとにライセンスト提供側で生成される一時鍵 共通鍵
	Ks2x セッション鍵	ライセンストの授受ごとにライセンスト受理側で生成される一時鍵 共通鍵
	KPcpy クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 [y]はクラスを識別するための識別子
	Kcpy クラス秘密鍵	クラス公開鍵KPcpyにて暗号化されたデータを復号する非対称な復号鍵
	lcpy クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cpy クラス証明書	$Cpy = KPcpy // lcpy // E(Ka, H(KPcpy // lcpy))$ 認証鍵KPaによってその正当性が確認できる
再生回路	Ks2x セッション鍵	ライセンストの授受ごとにライセンスト受理側で生成される一時鍵 共通鍵

FIG. 4

40

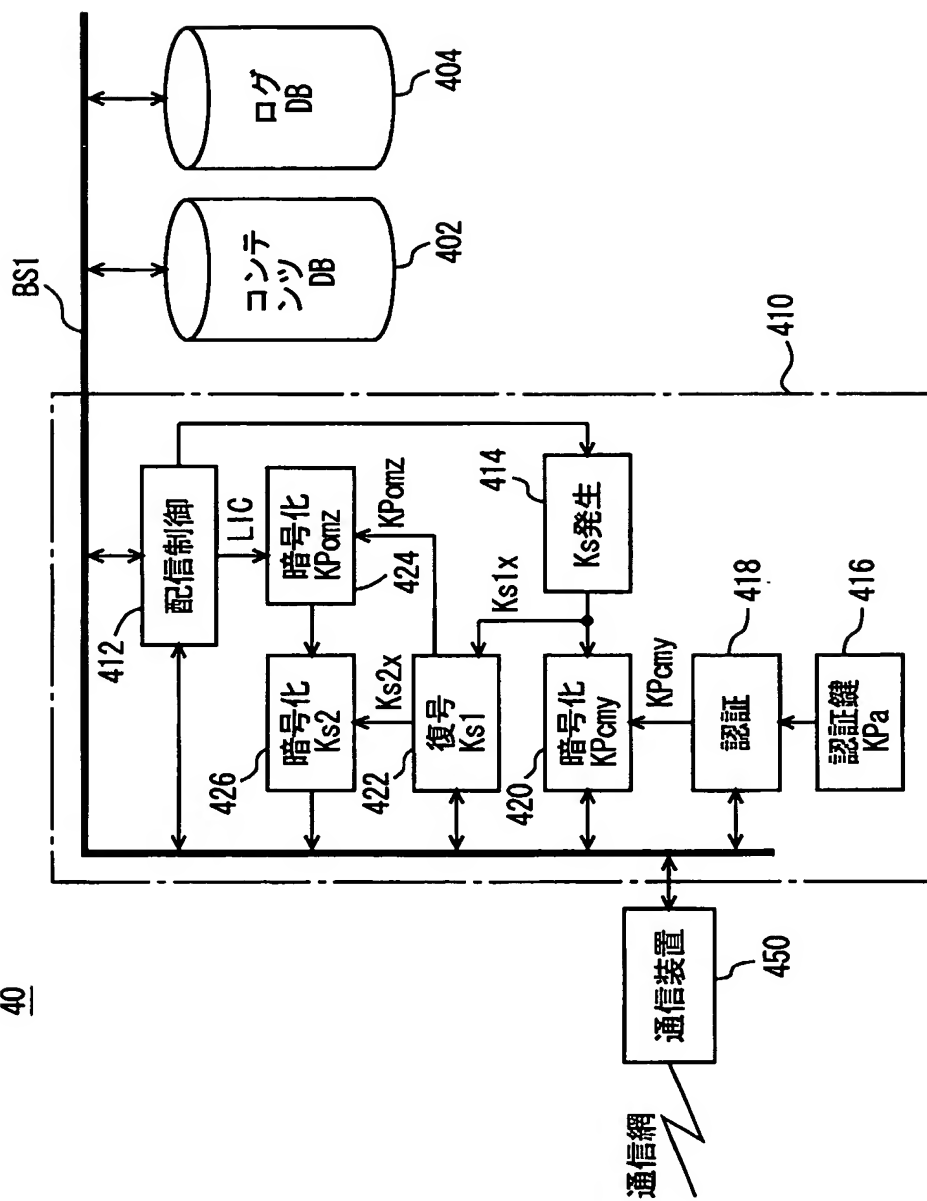


FIG. 5

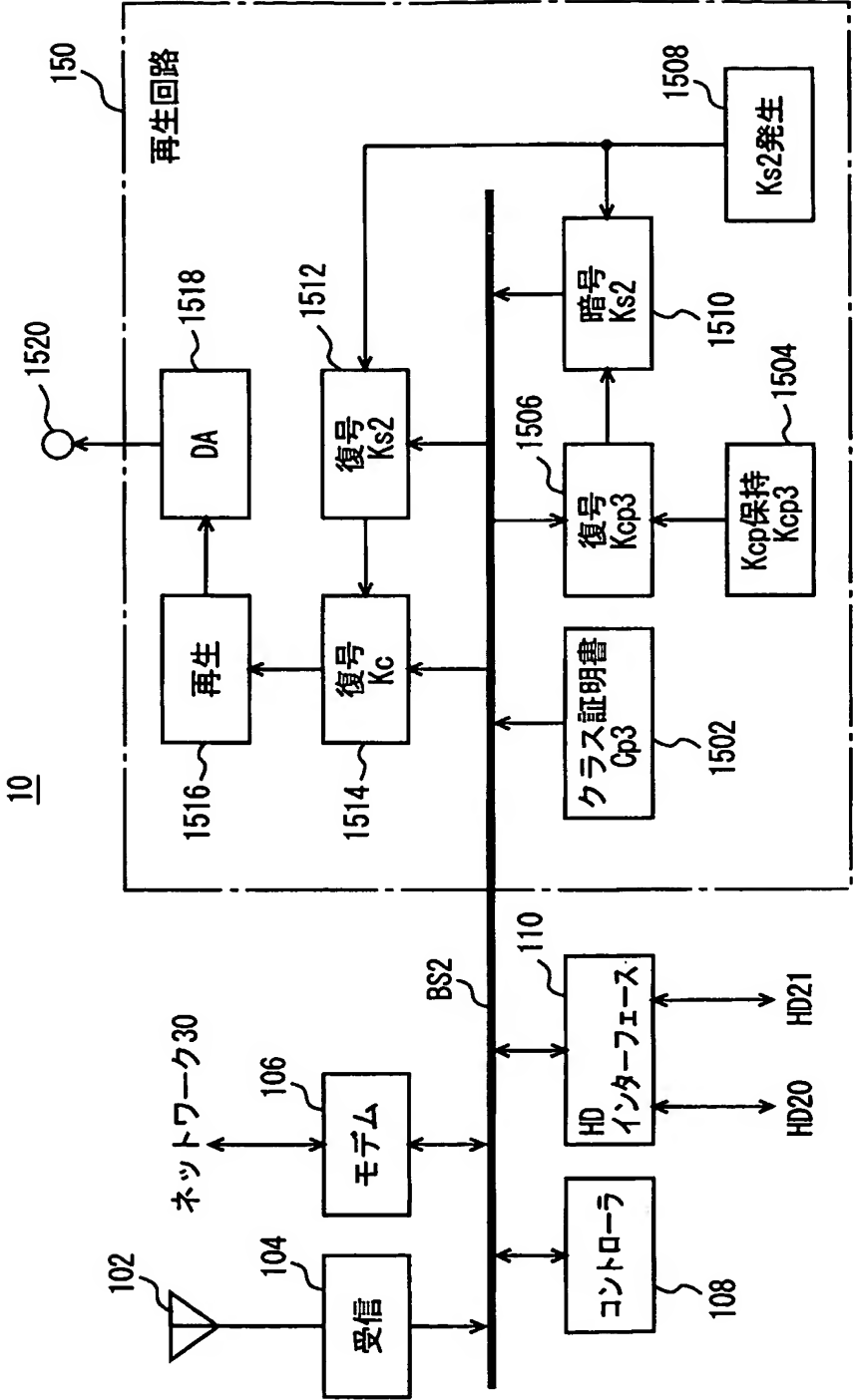


FIG. 7

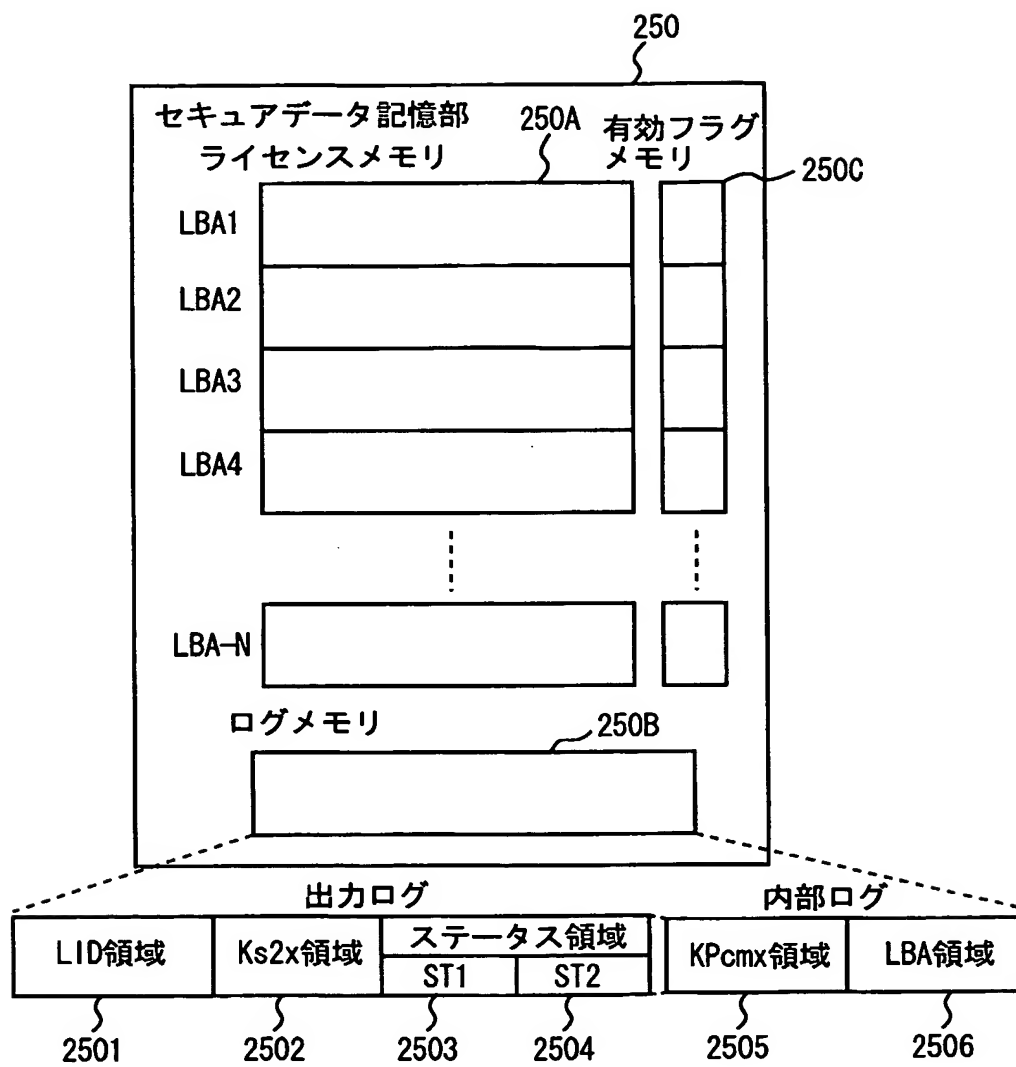


FIG. 8

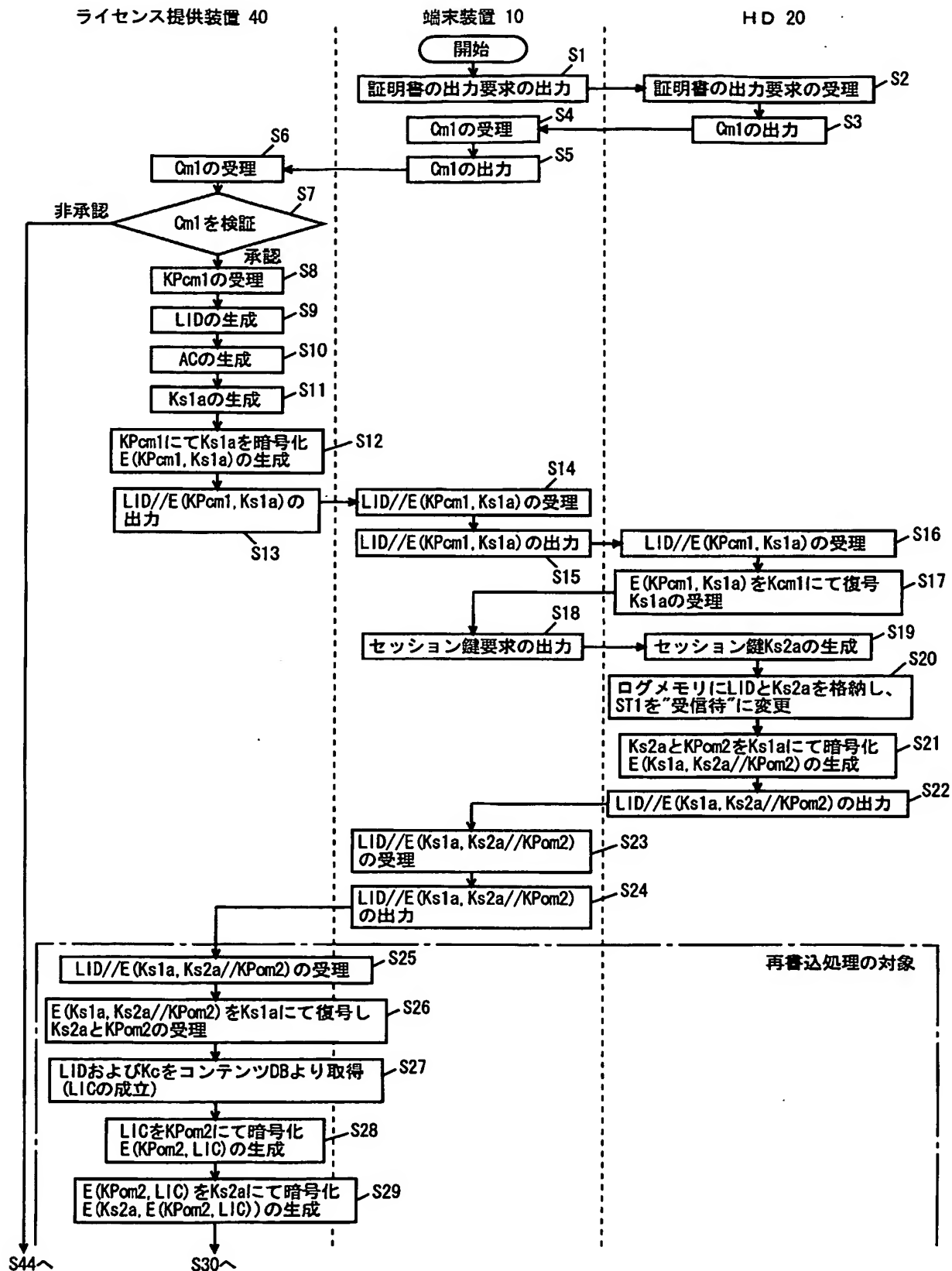


FIG. 9

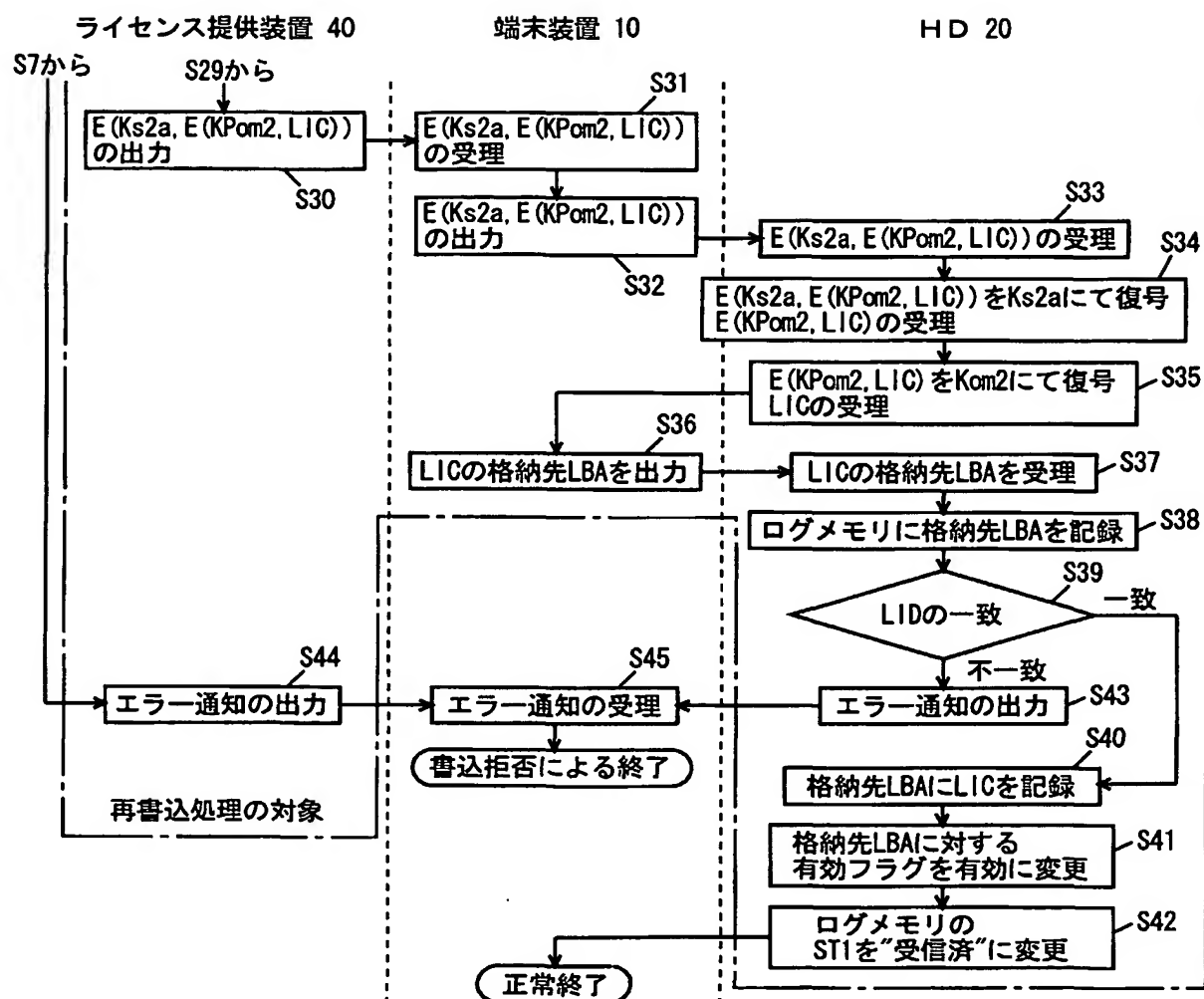


FIG. 10

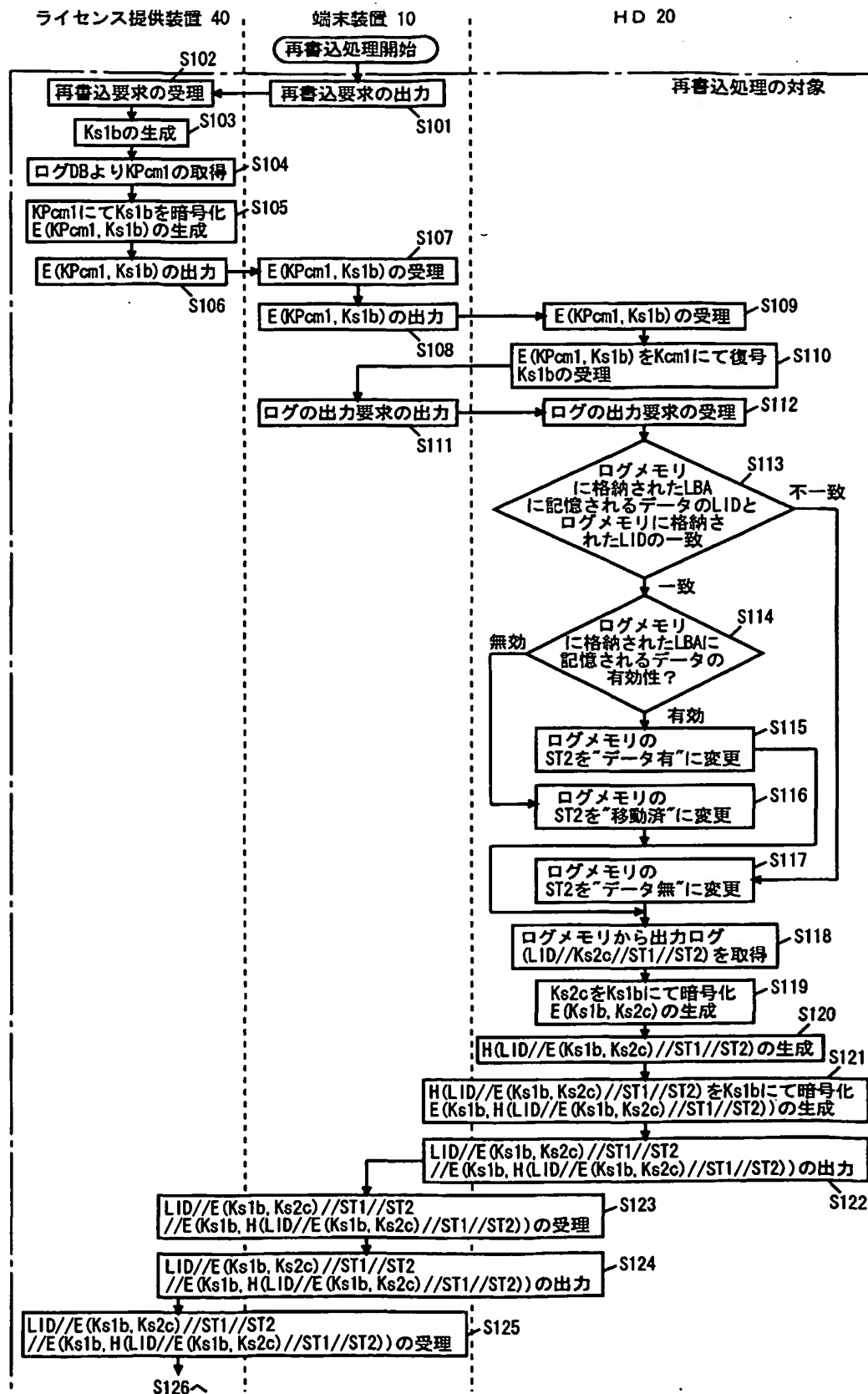


FIG. 11

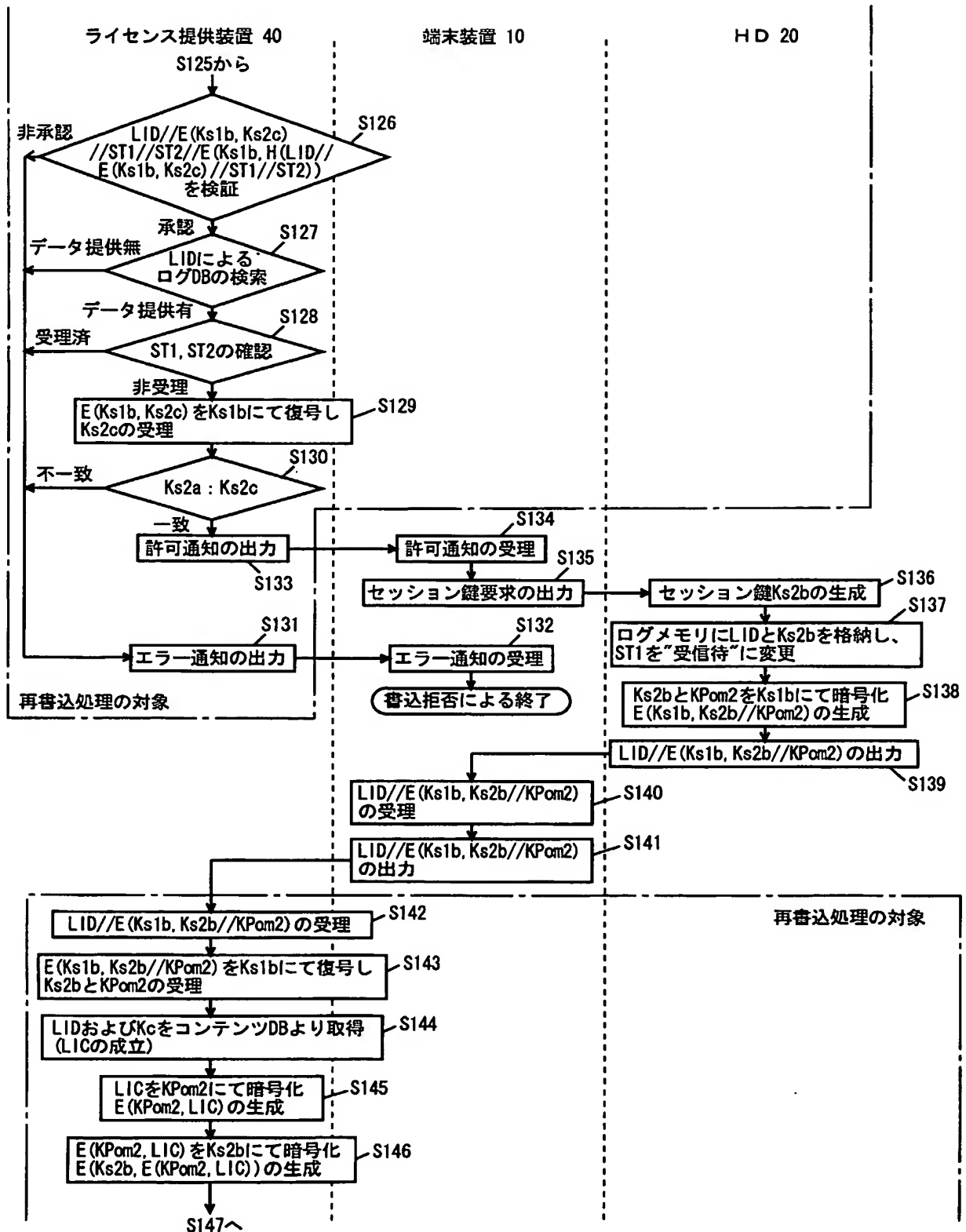


FIG. 12

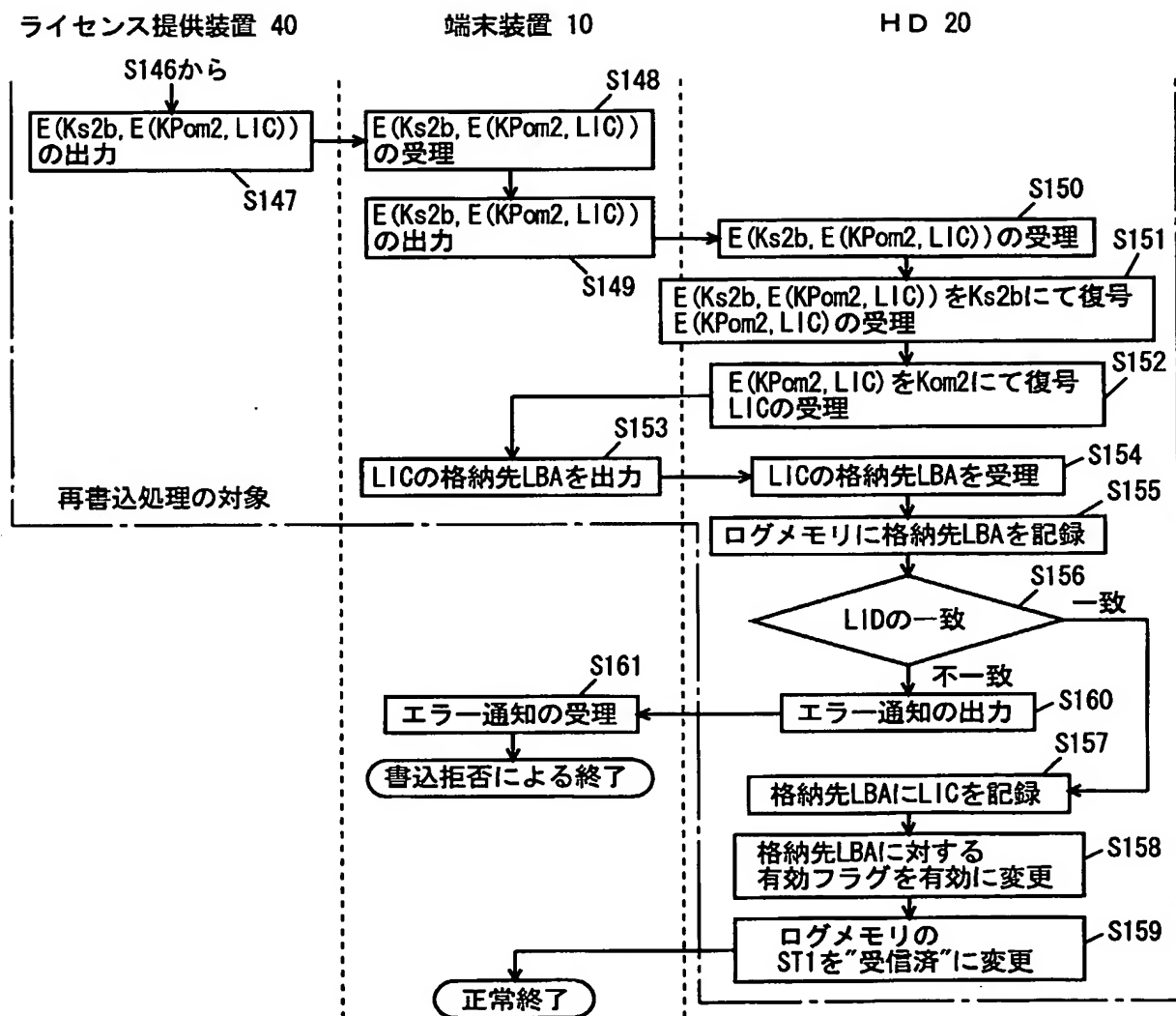


FIG. 13

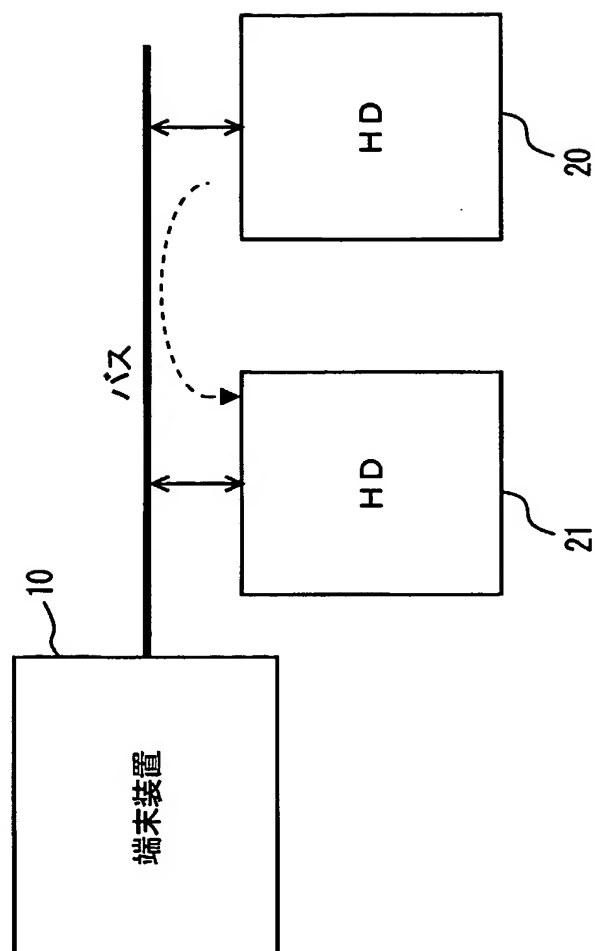


FIG. 14

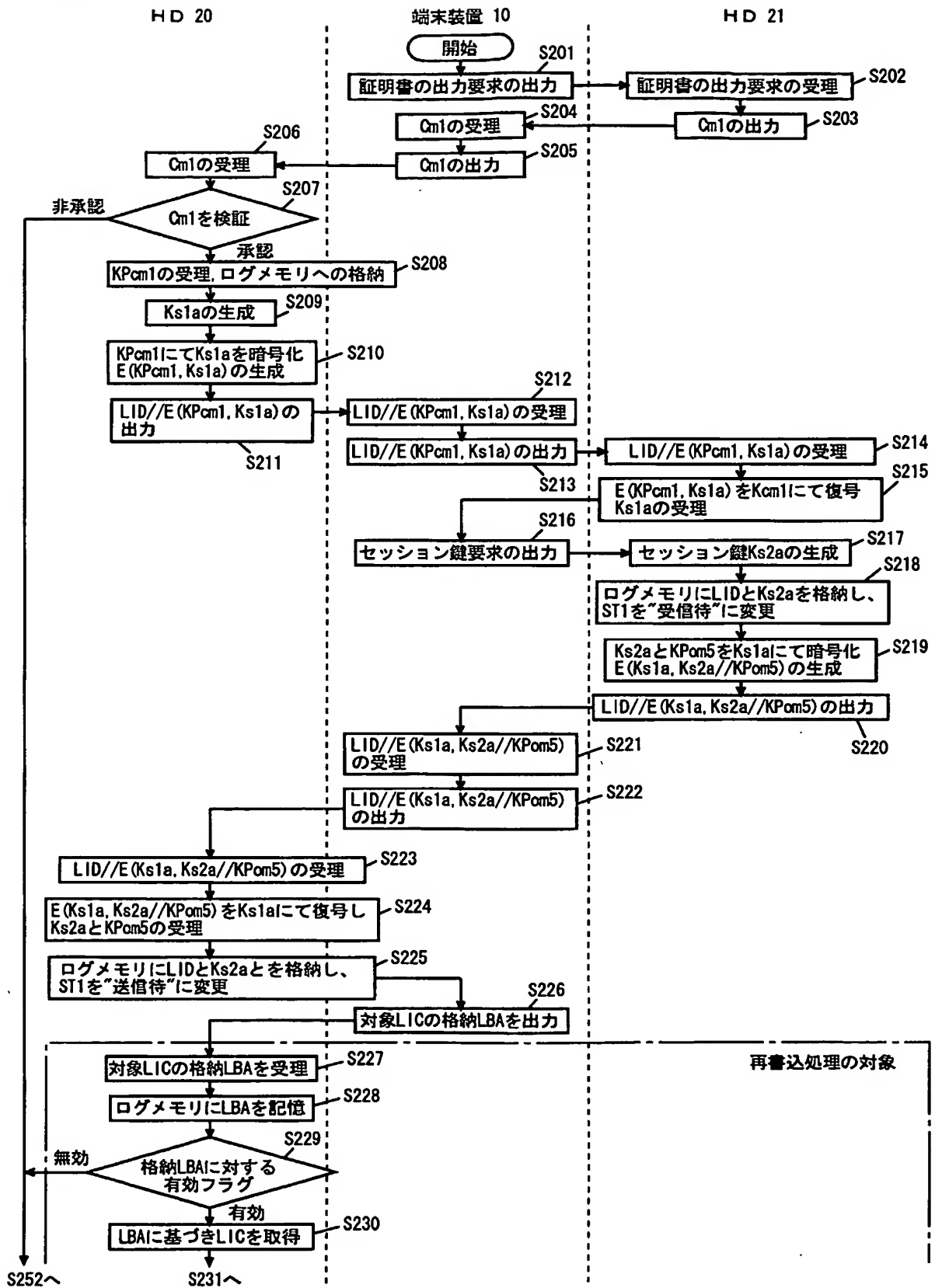


FIG. 15

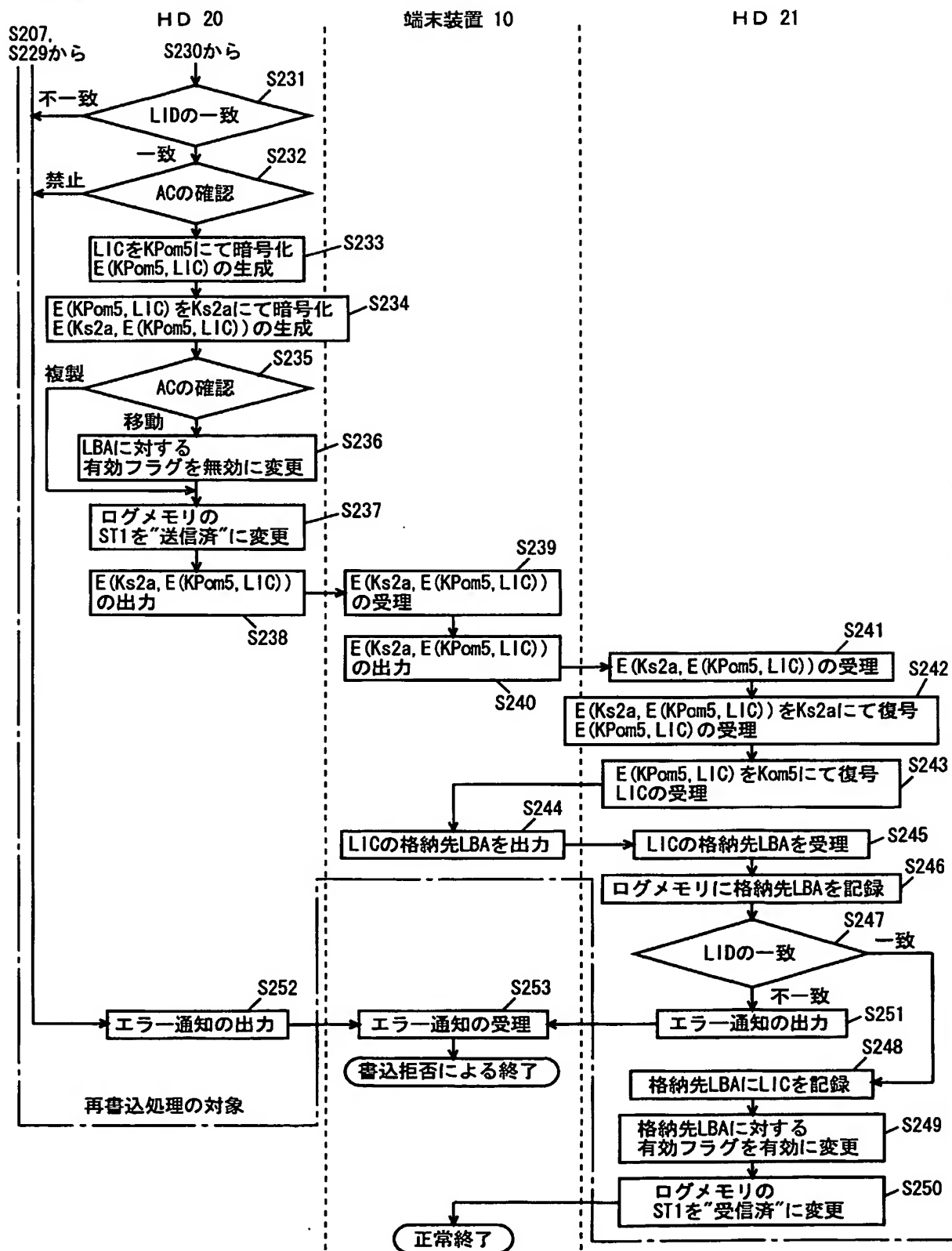


FIG. 16

HD 20

端末装置 10

HD 21

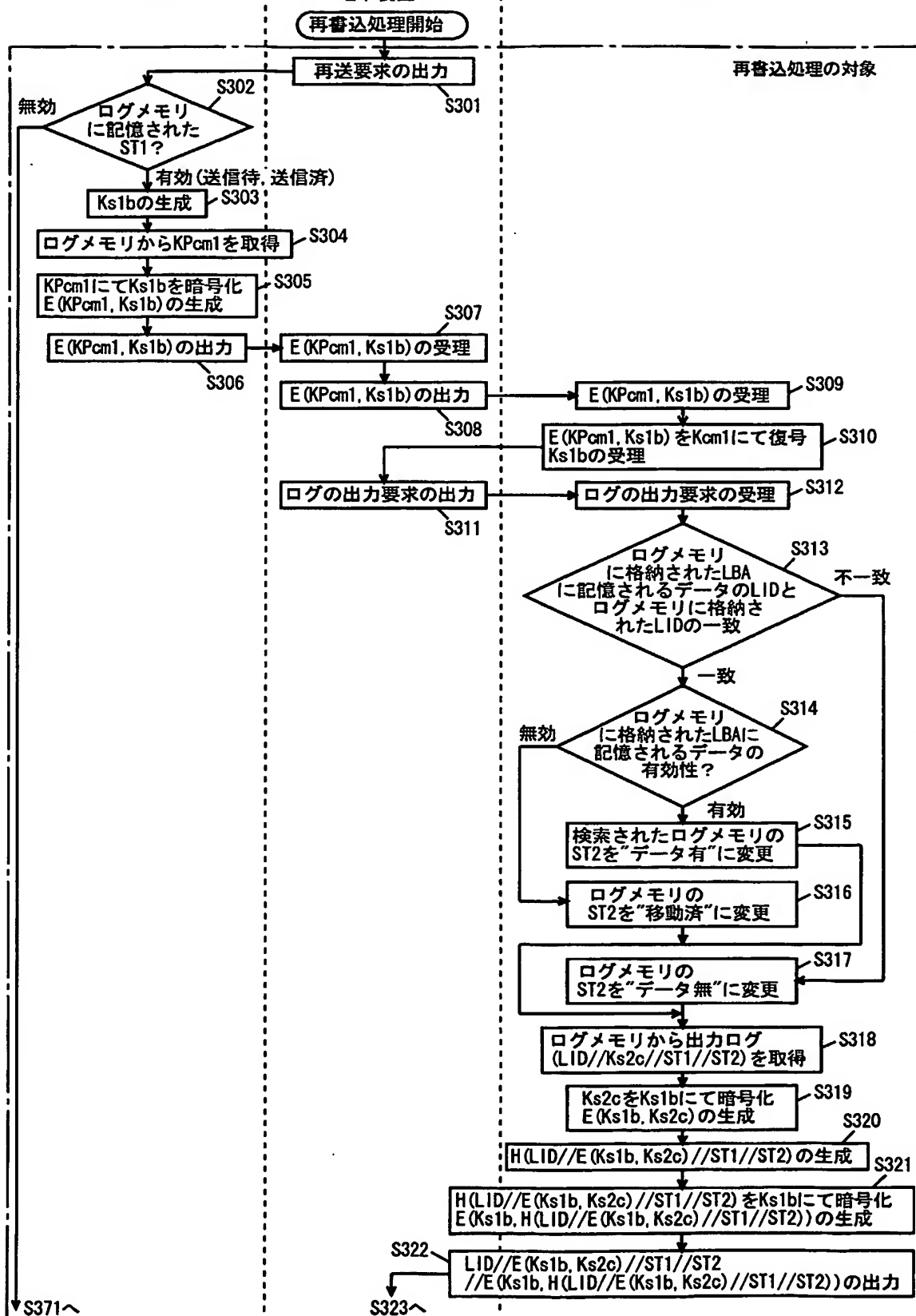


FIG. 17

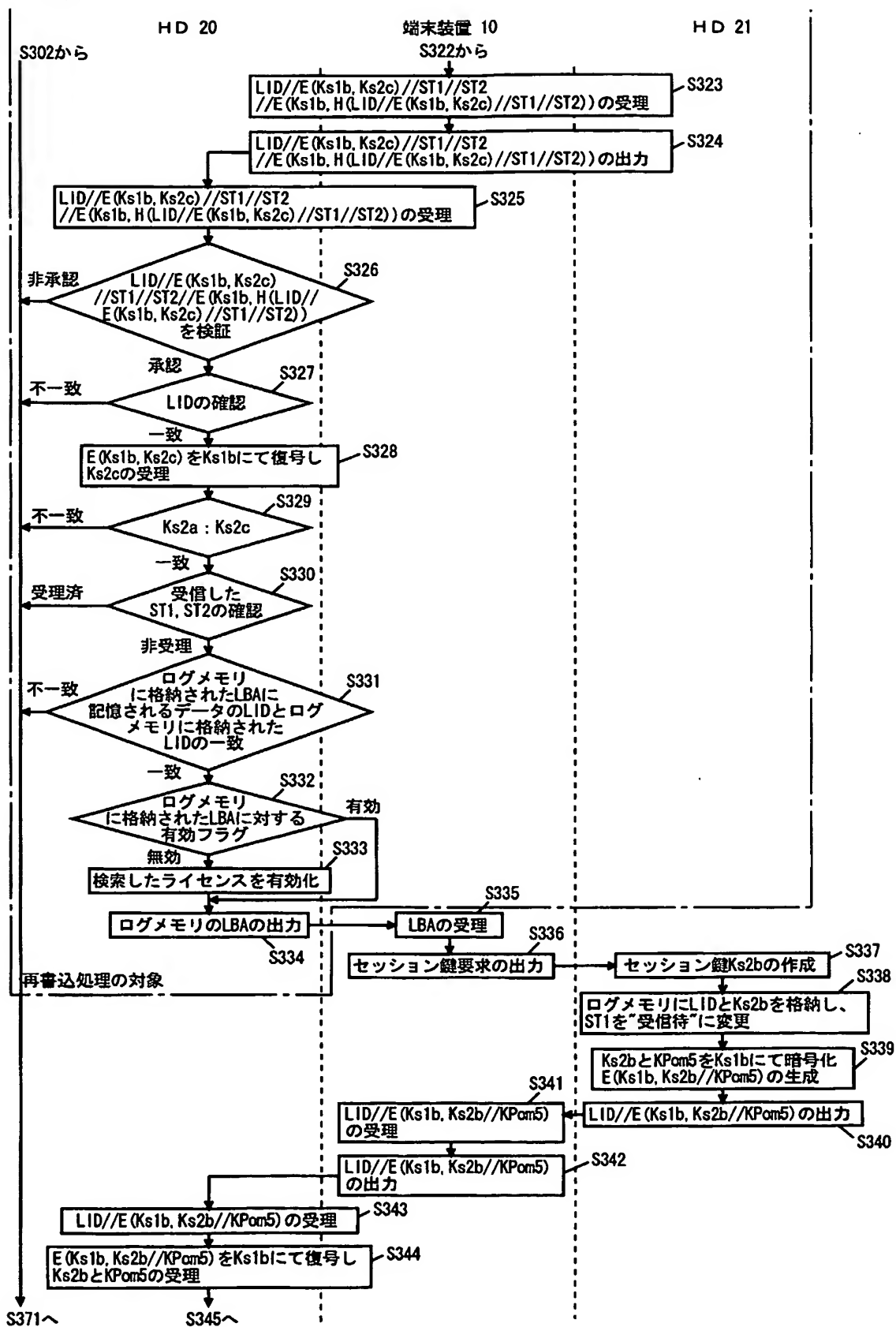


FIG. 18

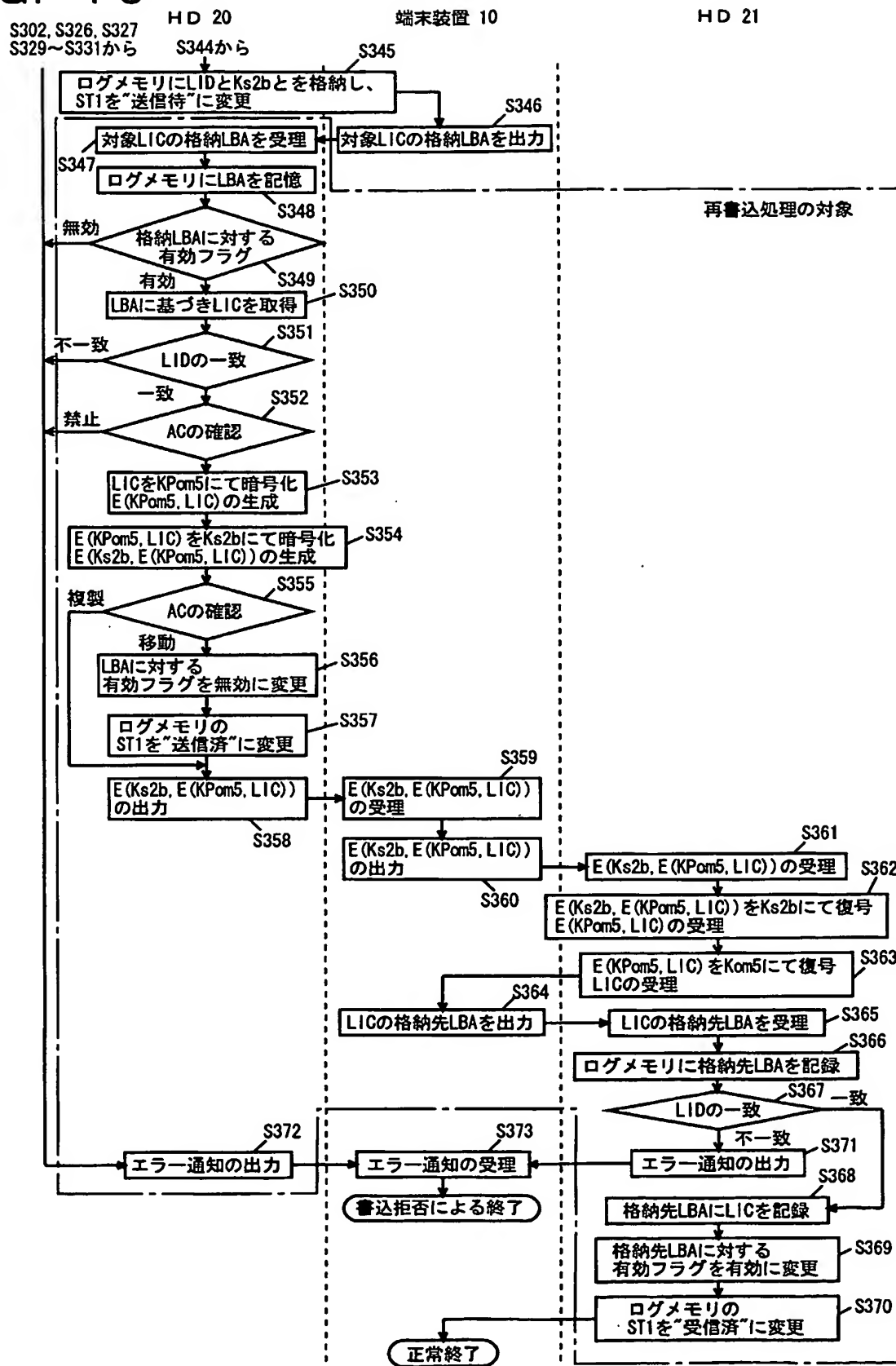
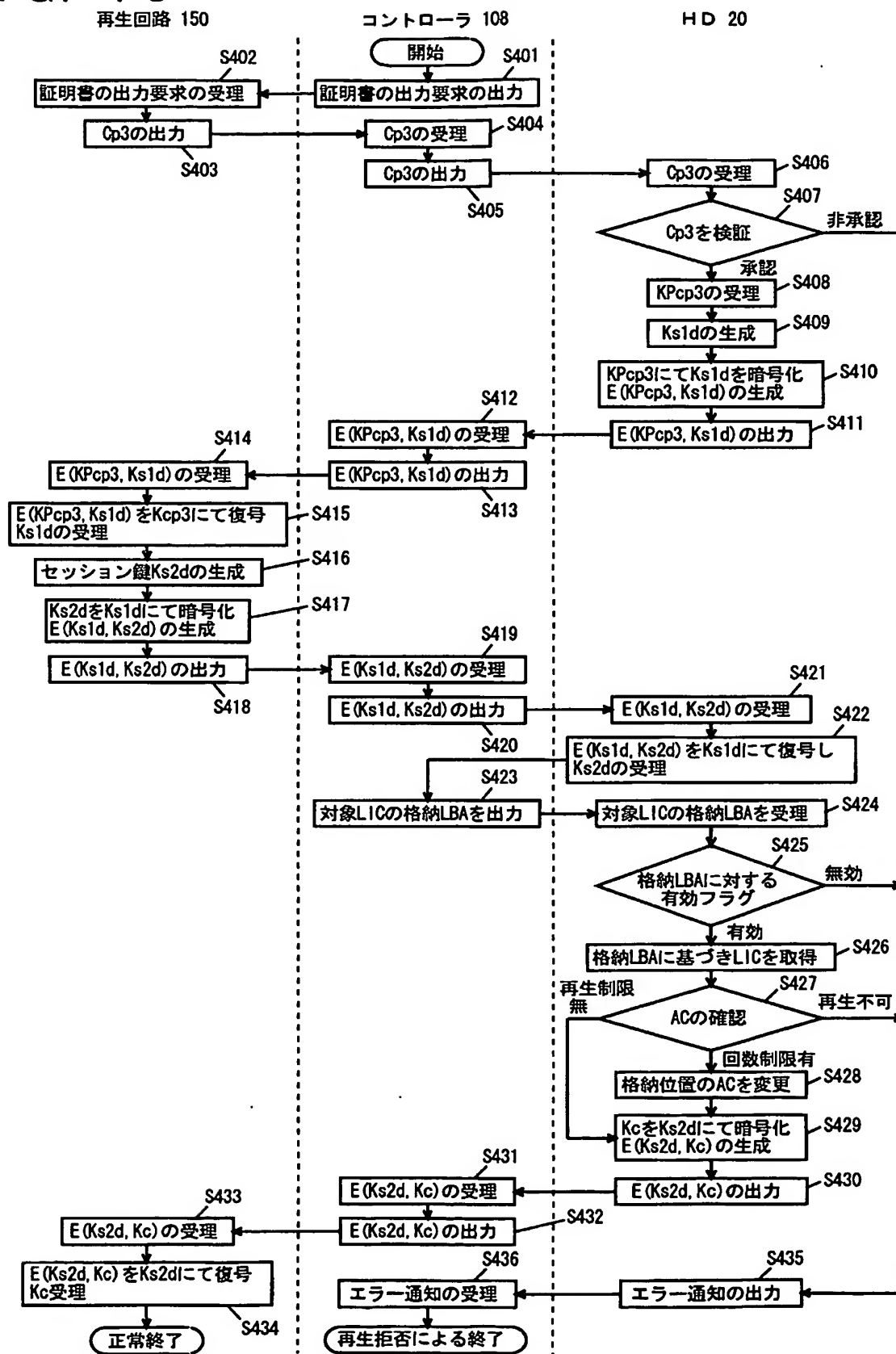


FIG. 19



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/02525

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F12/14, G06F3/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F12/14, G06F3/06, G06F12/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-230768 A (Sony Corp.), 24 August, 2001 (24.08.01), All pages; all drawings; particularly, abstract & WO 01/61911 A1	1-16
Y	JP 11-328982 A (Fuji Electric Co., Ltd.), 30 November, 1999 (30.11.99), All pages; all drawings; particularly, Fig. 2 (Family: none)	1-16
Y	JP 2001-147864 A (Seiko Epson Corp.), 29 May, 2001 (29.05.01), All pages; all drawings; particularly, Fig. 4 (Family: none)	2-15

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to
"A" document defining the general state of the art which is not considered to be of particular relevance	understand the principle or theory underlying the invention
"E" earlier document but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	"&" document member of the same patent family
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
21 May, 2003 (21.05.03)

Date of mailing of the international search report
03 June, 2003 (03.06.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/02525

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-240629 A (Mitsubishi Electric Corp.), 11 September, 1998 (11.09.98), All pages; all drawings; particularly, Fig. 1 (Family: none)	2-15
Y	JP 2001-249855 A (Hitachi, Ltd., Nippon Telegraph And Telephone Corp.), 14 September, 2001 (14.09.01), All pages; all drawings; particularly, Fig. 3 (Family: none)	2-15
Y	JP 2001-51889 A (Sharp Corp.), 23 February, 2001 (23.02.01), All pages; all drawings; particularly, Fig. 2 (Family: none)	2-15
Y	JP 2001-337600 A (Toshiba Corp.), 07 December, 2001 (07.12.01), All pages; all drawings; particularly, abstract (Family: none)	7,10,14,15
A	JP 9-69082 A (Toshiba Corp.), 11 March, 1997 (11.03.97), All pages; all drawings & EP 750260 A2 & CN 1147650 A & US 5828821 A & KR 247875 B	1-16
A	JP 10-3745 A (Sony Corp.), 06 January, 1998 (06.01.98), All pages; all drawings & EP 813194 A2 & CN 1182268 A	1-16
P,A	WO 02/75550 A1 (Sanyo Electric Co., Ltd.), 26 September, 2002 (26.09.02), All pages; all drawings (Family: none)	1-16

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F3/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F12/14, G06F3/06, G06F12/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926 - 1996
日本国公開実用新案公報	1971 - 2003
日本国登録実用新案公報	1994 - 2003
日本国実用新案登録公報	1996 - 2003

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 2001-230768 A (ソニー株式会社) 2001.08.24, 全頁, 全図, 特に【要約】 & WO 01/61911 A1	1-16
Y	JP 11-328982 A (富士電機株式会社) 1999.11.30, 全頁, 全図, 特に【図2】 (ファミリーなし)	1-16
Y	JP 2001-147864 A (セイコーエプソン株式会社) 2001.05.29, 全頁, 全図, 特に、【図4】 (ファミリーなし)	2-15

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

21.05.03

国際調査報告の発送日

03.06.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

原 秀人

5N

3044

電話番号 03-3581-1101 内線 3585



C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-240629 A (三菱電機株式会社) 1998.09.11, 全頁, 全図, 特に【図1】 (ファミリーなし)	2-15
Y	JP 2001-249855 A (株式会社日立製作所, 日本電信電話株式会社, 日立通信システム株式会社) 2001.09.14, 全頁, 全図, 特に【図3】 (ファミリーなし)	2-15
Y	JP 2001-51889 A (シャープ株式会社) 2001.02.23, 全頁, 全図, 特に【図2】 (ファミリーなし)	2-15
Y	JP 2001-337600 A (株式会社東芝) 2001.12.07, 全頁, 全図, 特に【要約】 (ファミリーなし)	7, 10, 14, 15
A	JP 9-69082 A (株式会社東芝) 1997.03.11, 全頁, 全図 & EP 750260 A2 & CN 1147650 A & US 5828821 A & KR 247875 B	1-16
A	JP 10-3745 A (ソニー株式会社) 1998.01.06, 全頁, 全図 & EP 813194 A2 & CN 1182268 A	1-16
PA	WO 02/75550 A1 (三洋電機株式会社) 2002.09.26, 全頁, 全図 (ファミリーなし)	1-16

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.